LÁNG BENEDEK

A rejtjelezés technológiájának használata Magyarországon az 1700 körüli években*

Feltűnő az ellentét a között az izgalom között, amelyet titkosírások szerepeltetése egyes regények olvasóiban kelt, valamint a között az érdektelenség között, amit az igazi titkosírások a történészben kiváltanak. Irodalmi, bestseller- és krimiszerzők hosszú sora kínál könyvében központi szerepet kódoknak és rejtjeleknek Edgar Allan Poe-tól *(Az aranybogár)* Isaac Asimovig *(1 to 999)*, Conan Doyle-tól *(A táncoló emberkék esete)* Agatha Christie-ig *(Négy gyanúsított)*, Edgar Wallace-tól *(Code No. 2)* Umberto Ecóig *(A Foucault-inga)*, Jules Verne-től *(A kriptogram)* Dan Brownig *(A da Vinci kód)*, Dorothy Sayers-től *(Have his Carcase)* Ken Follettig *(Kulcs a Manderley-házhoz)*.[1] A *Cryptologia* című titkosírás-történeti folyóirat minden számában recenzálja az újonnan megjelent, témába vágó szakkönyveket, és a recenziók közé a *„fiction"* kategóriában regényekről, krimikről is hasznos leírást ad.[2] Egy friss vizsgálat százötven olyan – viszonylag jól ismert – regényt sorol fel, amelyben titkosírások fontos szerepet játszanak.[3]

E népszerűséggel éles ellentétben maguk a fennmaradt történelmi titkosírások meglehetősen egyhangú benyomást keltenek. Egy rejtjelezett levél valójában semmi más, mint jelek vagy számok sorozata. Ha pedig nemcsak a jeleket és a számokat látjuk – vagy azért, mert a valamikori címzett a megfejtést a számok fölé írta, vagy pedig azért, mert ma egy ügyes kutató feltörte a kódot, és rekonstruálta a titkosíráskulcsot –, hanem a levél tartalma is olvashatóvá válik, meglepően kevés esetben nyerünk olyan információt, amelyet az adott korszak történészei már rég ne tudtak volna.

E tanulmányban azt kívánom bemutatni, hogy a késő 17. és kora 18. századi titkosított szövegek vizsgálata más szempontból is releváns. Túl az elrejtett üzenet tartalmán, gazdag információforrásává válnak a kornak, amelyben készültek. Figyelmes olvasóként közel kerülhetünk a felhasználók attitűdjeihez, a titok fogalmához, a technológia használatának részleteihez. Az alábbiakban kizárólag a rejtjelezésnek mint technológiának a használatára koncentrálok, a kriptográfia társadalomtörténeti hátterét és forrásanyagát más publikáci-

* Kutatásaimat az OTKA K 101544 támogatta, a cikket a Collegium de Lyon vendégszeretetét élvezve írtam. A nyomtatott források kivonatolásában Kálmán Dániel megbízható munkájáért mondok köszönetet, a levéltári források közt Sunkó Attila segített eligazodni. Szintén megköszönöm Cieger András, Farkas Gábor Farkas, Fazekas István, Kasza Péter, Kerekes Dóra, Pálffy Géza és R. Várkonyi Ágnes értékes tanácsait.

[1] *Dooley*, John F.: *Codes and Ciphers in Fiction: An Overview*. Cryptologia, 29. (2005) 290–328.

[2] http://www.tandfonline.com/toc/ucry20/current

[3] http://www.staff.uni-mainz.de/pommeren/Kryptologie/Klassisch/0_Unterhaltung/Lit/

ókban mutatom be.[4] A kérdéskörhöz korábbi kutatók fontos publikációit is ajánlhatjuk a hazai szakirodalomból.[5]

„Követett volna azon clavisokkal írott titkos mysteriumában"[6]

A kora újkori diplomáciai, politikai és hadi levelezésben visszatérő téma a titkosíráskulcsok használata, cseréje, javítása és a használatukból fakadó problémák kezelése. Rendszerint a levél legelején vagy a vége felé tesznek sifrírozásra vonatkozó explicit megjegyzéseket a levélírók, itt utalnak arra, mi működik, és mi nem, s itt adnak egymásnak visszajelzést a megkapott és meg nem kapott levelekről is. Ében István Teleki Mihálynak írt levelében például rögtön a második mondatban visszajelzi, hogy a levelezőpartnere levele és titkosíráskulcsa is megérkezett: „Mint jóakaró uramnak, Kegyelmednek szolgálok. Kegyelmed levelét ez elmult napokban az onnat jött officér megadá az clavissal együtt."[7] Bánffy Dénes szintén Telekinek írt levelében ugyancsak az első mondatokban utal a köztük folyó (ezúttal meglehetősen elhanyagolt) levelezésre: „Szolgálok Kegyelmednek. Igazán, Uram, az Kegyelmed igéreti is az Dunában esének, öt héttől fogva egy levelét láttam Kegyelmednek, azt is az fejedelemasszony kezéhez küldvén, nem régen akadt kezemben és hogy valami particulát az új clavissal írt Kegyelmed, Isten tudja, micsoda suspiciot vött Kemény Simon uram." Majd külön papíron magyarázkodik, amikor kiderül, hogy Teleki több levelet írt, mint amennyiről ő tud: „Ma reggel írván Kegyelmednek ezen levelemet, akada azután ismét Kegyelmednek egy levele kezembe, melyet, Bethlen Gergely uramra szerencsére akadván egy parasztember tegnap itt Cseke táján, ki vitte volna az fejedelemasszonynak, ő kegyelme elvötte, abból látom, hogy írja Kegyelmed, hogy nekem sokszor írt. Nekem bizony egy levelénél többet Kegyelmednek nem adták, most is, mint levelemben írám, Kegyelmedé az vétek."[8]

Milyen szavakat használnak a levélírók, amikor a titkosírásokról írnak? Míg a 19. századi szövegkiadások szerkesztői a „rejtelmes jegy" (rejtelmesen), „titkos jegy" (titkos jel, tit-

[4] A kérdéskör áttekintéséhez és a gazdag forrásanyag bemutatásához lásd: Láng Benedek: *People's secrets: Towards a social history of Early Modern cryptography*; megjelenésre elfogadva: The Sixteenth Century Journal, 2014.; uő: *Az emberek titkai: A rejtjelezés társadalomtörténete Magyarországon*. Korall, 43. (2011) 174–189. A kézirattárakban fellelhető és szövegkiadásban megjelent forrásanyag módszeres vizsgálatát készülő monográfiámban mutatom be: Titkosírás- és kódhasználat a kora újkori Magyarországon: a titok és a rejtjelezés társadalomtörténete (1500–1711).

[5] A teljesség igénye nélkül: R. Várkonyi Ágnes: *A tájékoztatás hatalma*. In: Petercsák Tivadar – Berecz Mátyás (szerk.): Információáramlás a magyar és török végvári rendszerben. Eger, 1999. 9–32.; uő: *A rejtőzködő murányi Vénusz*. Budapest, 1987. 213–215.; uő: *Az elveszett idő: Zrínyi Miklós nádori emlékirata?* Hadtörténelmi Közlemények, 113. évf. (2000) 2. sz. 269–328., különösen: 291.; Ötvös Ágoston: *Rejtelmes levelek első Rákóczy György korából*. Kolozsvár, 1848.; Révay Zoltán: *Titkosírások. Fejezetek a rejtjelezés történetéből*. Budapest, 1978.; uő: *II. Rákóczi Ferenc és korának rejtjelezése (XVIII. század)*. Budapest, 1974.; Tusor Péter: *Pázmány bíboros olasz rejtjelkulcsa: C. H. Motmann ‚Residente d'Ungheria': A római magyar agenzia történetéhez*. Hadtörténelmi közlemények, 116. évf. (2003) 2. sz. 535–581.; Vámos Hanna: *Leleplezett titok: Pálóczi Horváth Ádám titkos, szabadkőműves dokumentuma*. In: Csörsz Rumen István – Hegedüs Béla (szerk.): Magyar Arión Tanulmányok Pálóczi Horváth Ádám műveiről. Budapest, 2011. http://rec.iti.mta.hu/rec.iti

[6] Bánffy Dénes 1659. október 1-jén Telekinek: *Teleki Mihály Levelezése, A Római Szent Birodalmi Gróf Széki Teleki Család Oklevéltára*. Budapest, 1905–1926. vols. 1–8. (a továbbiakban: Teleki 1–8) vol. 1. 438–440., 381. sz.

[7] Teleki 2. 253–254., 186. sz.

[8] Teleki 2. 379–381., 282. sz. idézet: 379.

kos betű) és olykor a *chiffre* (chiffríroz) kifejezésekkel illették a titkosírásokat, addig a 16–17. századi történelmi szereplők elsősorban a *clavis* (igeként: clavisál), másodsorban pedig a „cifra" (ciffra, czifra) szavakat használják, valamint – csakúgy, mint a szövegkiadók – a *„chiffre"*-et.

Kulcsmegosztás

A kora újkorban rejtjelezett levelezés nem működhetett anélkül, hogy a levelezőpartnerek titkosíráskulcsot, *clavis*t cseréltek volna. A kulcs rendszerint elfért egy összehajtogatott lapon. Minthogy minden levelezéshez legalább két kulcsra volt szükség (egyre a feladó kódolónak, egyre pedig a címzett dekódolónak), de gyakran a levelezést adminisztráló titkárnak is volt egy példánya, nem meglepő tehát, hogy számos kulcs több példányban maradt fenn.[9]

A történelmi szereplők gyakran tettek rá utalást, hogy megfelelő titkosíráskulcs nélkül nem képesek vagy nem hajlandók igazán komoly dolgokról írni. Hallgassuk ismét Bánffy Dénest, aki újra Telekinek ír (1668. május 19): „Egyébiránt nekem clavisom sem lévén, nem merek írni, mert ha elfognák, azt tudnák, urunkat, hazánkat árultuk el s azért sollicitálunk pénzt..."[10] Másutt ugyanő: „Az correspondentia clavis nélkül nem lehet, kit is el ne mulassa megküldeni."[11] II. Rákóczi Ferenc Vay Ábrahámnak 1711. december 11-én Gdańskból: „Clavis nélkül írni nem mervén..."[12] Bethlen János 1667. március 2-i levelében hangsúlyozza, hogy „egy levélre clavis alatt jól rábízhatják" a bizalmas információkat.[13]

Nem meglepő tehát, hogy a történelmi szereplők rendszeresen felszólítják egymást, hogy *clavis*sal írják a leveleket, ennek híján pedig – általában a kevésbé fontos szereplő a fontosabbtól – *clavis*ért folyamodnak. Teleki Mihály Nemes Jánosnak 1678. január 2-án ezt írja: „Édes Komám uram jobban s igazabban írjon a clavissal."[14] Bethlen Miklós 1678. június 11-én: „...ugyan is azt javallom, kivált derék dologról mind a két uton és clavissal ír-

---

[9] Ilyen kulcsok gyűjteménye számos levéltárban fennmaradt: Gévay Antal 19. századi másolatai az OSZK Kézirattárában a Magyarországgal kapcsolatos Habsburg diplomácia közel ötven 16. századi tábláját tartalmazza: OSZK. Quart. Lat 2254. A bécsi Haus-, Hof-, und Staatsarchiv gyűjteményébe tartozó Staatskanzlei anyagok közt többé-kevésbé ábécérendben közel kétszáz hasonló kulcs található: ÖStA HHStA Staatskanzlei Interiora Kt. 13-16. Chiffrenschlüssel. (Fazekas Istvánnak és Pálffy Gézának mondok köszönetet, hogy erre az értékes anyagra felhívta a figyelmem.) Teleki Mihály tíz *clavis*át a Teleki család Marosvásárhelyi Levéltárának MOLban őrzött anyagai közt lelhetjük fel: MOL P 1238 Teleki Mihály Gyűjtemény. Vegyes Iratok. Titkosírás kulcsok. A Wesselényi összeesküvés felszámolásakor lefoglalt titkosírások (huszonkét kulcs és öt titkosírt levél) szintén Bécsben találhatók: ÖStA HHStA Ung Act. Spec. Fasc. 327. Konv. D. Chiffres 1664–1668. A Rákóczi szabadságharc titkosírástábláit három jelzet alatt találjuk, kettő ezek közül a fejedelem levéltárának emigrációba vitt részére, a Rákóczi-Aspremont levéltár MOL-ban őrzött – és az 1956-os nagy pusztítástól, amely éppen a Rákóczi-anyagot tizedelte meg, szerencsére megkímélt – gyűjteményre vonatkozik: Mol G 15 Caps. C. Fasc 43 és 44, a harmadik pedig Ráday Pál irataira a Ráday Levéltárban: Ráday Levéltár C64-4d2-25. Kisebb – tíznél kevesebb kulcsot tartalmazó – gyűjtemények találhatók a Mednyánszky család levéltárában II. Rákóczi György és Mednyánszky Jónás levelezéséhez: MOL P 497 Mednyánszky Család, 3. csomó és Esterházy Pál levelei közt a MOLban: MOL P 125, *Esterházy* Pál nádor iratai, No. 119 772.

[10] Teleki 4. 297–298., 221. sz.

[11] Teleki 4. 461–463., 340. sz.

[12] *Archívum Rákóczianum, II Rákóczi Ferenc levéltára*. Budapest, 1873–1935) vols. 1–12. (a továbbiakban: AR I. oszt.) 3. köt. 698–701., 92. sz.

[13] Teleki 4. 47–49., 36. sz.

[14] Teleki 8. 4–5., 4. sz. (C.Tel.03)

jon Kegyelmed..."[15] Teleki Mihály 1678. február 15-én: „Rédei uram ott lévén, hogy titkosabban legyen az dolog, ő kgk írám meg clavissal. Istenért ki ne tudódjék."[16] II. Rákóczi Ferenc 1710. május 5-én Atányból Esterházy Antalnak: „Kegyelmed az postalis lineán curirok által folytassa leveleit, in casu necessitatis az újvári clavisekkel élvén."[17] Palkovics Ferenc 1709. augusztus 14-én Simontornyáról Bercsényinek: „Hahogy az ellenség jobban keről fog minket venni és sarkalni, claveseket csináltasson Ngod és úgy írjon ide bé nekünk."[18]

Dalmady István 1659. január 4-én Telekitől kér kulcsot: „Ha nem restelli, csináljon egy clavist titkos betűvel, írhassunk egymásnak nagyobb confidentiával."[19] Hasonló kéréssel fordul Vitnyédi István 1662. október 22-én Rohoncról Zrínyi Miklóshoz: „Ha tetszenék Ngdnak talán nem ártana egy clavist küldene Ngd, melylyel bizvásban írhatnék, mert ugy gondolom ezután occurrálnak oly dolgok, az melyeket szükségképen köll tudni Ngdnak."[20] Ugyanő, ugyanannak, kissé később, 1663. február 18-án Sopronból: „Ugy látom leszen nekem Ngdhoz való titkos írásra hamar nap szükségem, Ngdat alázatosan kérem, küldjön clavist, az mint Ngdtúl való búcsüvételem korán emlité Ngd, hadd írhassak bátrabban, az hozzám küldendő szolga hoz derekas oly dolgot, melyet meg köll írnom Ngdnak, másonnend is érkezik hasonló dolog."[21] A *clavis*-kérés oka mindig a jelentőséggel bíró és bizalmas természetű információ megosztásának a vágya, magyarul az, hogy egy történelmi szereplő igyekszik felajánlani a szolgálatait egy jelentőségben felette álló politikusnak, ezúttal Zrínyinek. Bármennyire is szeretne Vitnyédi titkos leveleket küldeni, arra természetesen nincsen lehetősége, hogy maga készítsen egy titkosíráskulcsot, és rávegye a bánt, hogy az ő *clavisát* használja.

A kulcsküldésre vonatkozó kérést vagy felszólítást gyakran tett követte, és a levelezőpartnerek *clavist* cseréltek egymással. Rákóczi írja 1706. július 21-én Senthe várából Eszterházy Antalnak levele utolsó mondatában: „Hogy pedig az correspondentia bátorságosabban meglehessen, imé, clavist küldök Kegyelmednek, az mellyel ha az egész levelet nem is, in casu interruptae et periculosae correspondentiae, az legszükségesebb dolgokat tudtomra adhatja Kegyelmed."[22] Kászoni Márton 1663. december 20-án levele végén így búcsúzik: „Ím új clavist küldtem Kegyelmednek. [...] Kegyelmed securus legyen abban, ha mi hírek lesznek, Kegyelmedet mindenekről tudósítom; kérem, Kegyelmed is azt cselekedje. Isten hozza Kegyelmedet jó hírekkel vissza."[23] Lippay György 1637. július 31-én Rákóczi György fejedelemnek írt levelét így kezdi: „Ngodnak az minapiban derék dolgokról írtam az havasali vajda emberétől és clavist is küldöttem. Elkésett nyilván valahol, mert eddig válaszomnak kellett volna jűni Ngodtúl."[24]

A *clavis* átadására több mód adódott. Gyakran egy levéllel együtt küldték meg, olykor külön futárral, esetleg – és ez számított a legbiztonságosabbnak – személyes találkozás során bonyolították le a cserét. Levélmellékletként küldi Lippay György 1637. július 16-án

[15] Teleki 8. 216–217., 178. sz.

[16] Teleki 8. 78., 68. sz.

[17] AR I. oszt. 3. köt. 253–257., 26. sz.

[18] AR I. oszt. 9. köt. 714–715., 538. sz.

[19] Teleki 1. 311–312., 278. sz.

[20] Magyar Történelmi Tár, (Pest (majd Budapest), Magyar Tudományos Akadémia, 1855–1934 (a továbbiakban: MTT) II/3. 237–239., 229. sz.

[21] MTT II/4. 37–41., 261. sz.

[22] AR I. oszt. 1. köt. 563–565., 82. sz.

[23] Teleki 2. 660–661., 453. sz.

[24] Beke Antal (szerk.): *Pázmány, Lippay és Eszterházy levelezése.* MTT III/5. 147., 35. sz.

Bécsből Rákóczi Györgynek, maga a *clavis* is fennmaradt:[25] „...kinek alkalmatosabb véghezvitelére im az clavist is megküldöttem Ngodnak. Volnának alkalmas dolgaim nekem is, melyeket örömest közlenék Ngoddal, de ezúttal még nem lehet, elvevén az clavist Ngod, akkor talán írhatok."[26] Rákóczi augusztus 26-án visszajelez, hogy megkapta: „Ez előtt négy nappal vévén el az havaseli vajda emberétől 16. Julii írott Kgd levelét mind az bele includált clavissal együtt...", [27] majd még egyszer, szeptember 19-én: „Ezelőtt négy héttel vettük vala az havaseli vajda emberétől 16. Julii irott Kid levelét mind az bele includált clavissal együtt."[28]

A *clavis* sikeres megérkeztének visszaigazolása más esetben is fontos volt, Teleki Mihály egyik *clavis*ának hátoldalán olvassuk az udvarias kérést: *„Rogo responsum an reciperit hanc cartam nisi duo verba."*[29] Ében István Teleki Mihályhoz intézett 1662. március 1-jei levelének első sorai mintha arra utalnának, hogy a kulcsot külön futár vitte el számára: „Kegyelmed levelére választ töttem volt, ha másfelé nem vitték, úgy hiszem, eddig Kegyelmednek kezéhez ment. Az clavist meghozták."[30]

Végül pedig két forrás is a személyes találkozót említi mint sajnálatosan kihagyott alkalmat, amikor kívánatos lett volna *clavis*t cserélni. Bercsényi Miklós kezdi így a levelét 1710. október 26-án: „Elfelejtettem Eszterház Antal Uram clavisét elkérnem Fölségedtül."[31] Rédei László 1660. augusztus 31-i, Husztról írt levelét érdemes hosszabban is idézni, mert zavarosságában és bonyolultságában is jól mutatja, mennyire nehézkes volt olykor a titkosírás-használatról folyó egyezkedés, mennyire könnyen adódhatott, hogy egyik történelmi szereplő nem értette tisztán a másik szándékát: „Sokszor megbántam, hogy urunkkal létemkor, ő nagyságától clavisról való informatiot nem vöttem volt, de akkor meg sem gondoltam, hogy így történjenek az állapotok; magam sem tudtam ugyan eddég, hanem most tanúlom, de mi haszna, ha urunk nem tudja az én clavisomot. Kegyelmednél azért talám lehet és ha nincs is, talám meg írhatja ezeket a szókat clavissal; ha penig nincsen kegyelmednél is, s nem írhat ő nagyságának clavissal, ha bátorságos, ez kegyelmednek szólló levelemet küldje be kegyelmed ő nagyságának, talám be is küldheti, mivel én csak azt írtam urunknak ő nagyságának, de azt sem írtam meg, hol legyen kegyelmed, hogy ő kegyelmének írtam egynihány szót, kit nagyságod ő kegyelme clavissal írt meg, mivel én nem tudom. Így lévén azért a dolog, ő nagysága az én levelemből semmit nem érthet, hanem ha vagy ezen levelet küldi be kegyelmed ö nagyságahoz, vagy penig clavissal írja meg ez egynihány szót (itt következik a titkosítva továbbítandó levél)."[32]

Miután a megfelelő *clavis*ok elküldettek, átadattak és gazdát cseréltek, a levelezőpartnerek használatba vették őket. Ekkor azonban újabb probléma adódott. Hogyan lehet megnevezni az egyes titkosíráskulcsokat? Minthogy egy komolyabb politikai szereplő számos viszonylatban folytatott titkos levelezést, és ezáltal számos különböző kulcsot kezelt, valahogyan meg kellett különböztetni ezeket. A megnevezés leggyakrabban a feladó vagy a címzett nevét használta, feltételezve (olykor okkal, olykor ok nélkül), hogy az illető csak egy irányban folytat titkos levelezést. A levélíró gyakran a részlegesen vagy teljesen titkosított

[25] Kiadva: MTT III/5. 146., 34. sz.
[26] MTT III/5. 144–146., 34. sz.
[27] MTT III/5. 280–281., 37. sz.
[28] MTT III/5. 283–284., 39. sz.
[29] MOL P 1238 Teleki Mihály Gyűjtemény. Vegyes Iratok. Titkosírás kulcsok
[30] Teleki 2. 259–260., 189. sz.
[31] AR I. oszt. 6. köt. 609–610., 54. sz.
[32] MTT II/5. 101., 25. sz.

levél után, az aláírás és a dátumozás alatt specifikálta, hogy melyik eszközt használta. „Ezt Uram Szalai uramnál való clavissal irtuk."[33] „Kegyelmednek ezen levelünket Gróf uram clavissával írtuk."[34] „Absolon uram clavisával írtam."[35] „Fajgel uram clavissával írtam Uram Kegyelmednek."[36] „Ezen levelet Kegyelmed régi clavisával írtam."[37] „Az egész leveleket Kegyelmed Faigel urammal levő clavissával irattam."[38] Alkalmanként a levél belsejében is specifikálni kellett egy *clavis*t, ilyenkor is a felhasználó nevét használják. Nemessányi Bálint írja: „...nem lévén még nálam Absolon urammal való clavissa Kegyelmednek nem referálhattam..."[39]

Máskor körmönfontabban írják körül a kulcsot: „Az neveket azon clavissal írtam Kemény Simon uramnak, kit Kegyelmed küldött, nem tudom, tudja-e, nem-e? tudósítsa Kegyelmed."[40] „Az mely clavist Kegyelmed nekem csinált az abczére, arra írt az öcsém Kegyelmednek, ha mikor ír Kegyelmed, csak arra írja."[41] Csak remélni tudjuk, hogy Kemény János értette, amikor Mednyánszky Jónás így magyarázta, melyik rendszerrel sifrírozza a levelét: „Urunknál levő clavisból Nagysága ezeket megértheti."[42] Minthogy a levél titkosított részei máig sincsenek feloldva, azt sejthetjük, hogy a valamikori címzett sem volt kisegítve a homályos meghatározással.

A kulcsmegosztás tehát visszatérő igény volt, a gyakorlatban azonban gyakran adódtak problémák. Rákóczi 1710. július 19-én Tatárszentgyörgyről Bercsényinek írt levelében kétszer is kitér a *clavis*okra. Először szemrehányást tesz a fővezérnek, hogy levelében túl kevés tartalmat titkosított, és illetéktelenek is elolvashatják a levél bizalmas tartalmát („nem ártott volna, ha abban az melyben kegyelmed az negóciátiókról ír, több clavis lett volna, mert parasztemberek által gyűnek ide Szolnokbúl az levelek [...] de az tolvajoktúl nem mindenkor bizonyos járások"), majd pedig arról ír, hogy egy levélnek „nem fejthette ki clavisát, mert nállam nem maradt copiája".[43] Máskor mindkét fél birtokában van ugyan a megfelelő *clavis*nak, de az hibás. Hibás *clavis*sal márpedig nem lehet írni, ahelyett másikat kell küldeni, de az új *clavis* megérkeztéről ismét meg kell bizonyosodni. Teleki Mihály írja Naláczi Istvánnak 1678. január 15-én: „Az mely clavist ott hagytam, felette igen bajos vele írni, sok híjja lévén az bötükben. Ím mást küldöttem, de ezzel addig nem írok, míg Kegyelmed meg nem írja, hogy elvette és levelemet felszakasztás nélkül vette el, kirül kérem tudósítson. Az étekfogót jól megkérdezze, nem volt-é valaki kezénél levelem."[44] Rákóczi – nyilván a technológiahasználatban való személyes érintettsége folytán – számos alkalommal említ kulcsmegosztásból adódó problémákat. 1708. március 11-én Kassáról írja Bercsényinek: „Az feleségem is írja, hogy Urbich most már az cár követje lévén, offeráltatta titkos szolgálatját és correspondentiáját, valóban szeretném is, ha lehetne valamely módot kigon-

[33] Teleki 8. 249., 222. sz., 1678. szeptember 4.
[34] Teleki 8. 265–266., 238. sz. 1678. szeptember 13.
[35] Teleki 8. 433–435., 413. sz. 1679. április 27.
[36] Teleki 8. 68–69., 63. sz. 1678. február 9.
[37] Teleki 8. 528–530., 518. sz. 1679. szeptember 27.
[38] Teleki 8. 327–328., 304. sz. 1678. november 12.
[39] Teleki 8. 141., 125. sz. 1678. április 7.
[40] Teleki 2. 262–264., 193. sz.
[41] Teleki 1. 389–390., 342. sz. 1659. április.
[42] MTT II/6. 86–89., 48. sz. 1655. júl. 16.
[43] AR I. oszt. 3. köt. 133–137., 84. sz.
[44] Teleki 8. 19–20., 20. sz.

dolni az clavis transmissiójában."[45] 1710. január 16-án Tótfaluból megint Bercsényinek: „Szluha clavisos levelét silabizálván tél-túl: úgy tetszik, vólnának oly dolgok benne, az mellyeket jó volna tudnom, – de nem vólt clavisom hozzá, Kegyelmedtúl is későn fog idekerülni magyarázatja."[46] 1711. május 26-án Zalusáról Sennyei Istvánnak: „Mivel Kegyelmed most is ollyan clavissal ír, a mellyet praevie megmondottam vala, hogy Károlyinál is megvan, – nem lévén bizonyos abban: ha nem tévelyedett-é el az, a mellyet Vay úr tabellában resignált Kegyelmednek? még bizonyos nem leszek, hogy kezénél vagyon, több particularitásokat Kegyelmednek nem írhatok."[47] Kemény János ötven évvel korábban, 1658. ápr. 10-án így rendelkezik egy elveszett kulcs pótlásáról: „Az mely clavist küldtem volt, talám Radulyék elvesztették azt is, most újabban vigye meg Szigeti uram."[48]

A kulcsmegosztásba Lippay György érsek és Rákóczi György fejedelem 1637-es levelezésébe is hiba csúszott: a fejedelem hibát talál az érsek számára megküldött *clavis*ában, mire Lippay, aki maga nem találja a hibát, kissé indignálódva azt kéri, javítsa már ki gyorsan, és használják az új, kijavított kulcsot: „Az minemű clavist küldöttem, avval sem akart élni eddig Ngod, utoljára talált valami fogyatkozást benne, az kit én még most sem tapasztalok, de ha volna is, könnyen kedve szerint meg corrigálhatja Ngod, megküldvén az mássát énnekem is, talán eddig nem volt szintén haszontalan az én vékony munkám és szolgálatom az Ngod dolgaiban, bánnám ha Ngod az én jó szándékommal és confidentiámmal megbántódnék ezután is."[49] Három nappal később megismétli kérését: „Az clavisról írtam az curier által, corrigálja meg Ngod az miben kétes, és cum correctione küldje meg én nekem az mássát."[50]

Minden hibát nem lehet elkerülni, mégis példás Bethlen Miklós óvatossága, aki 1672. március 14-i levelében nemcsak a kulcsmegosztásról rendelkezik, de arról is, hogy mi a teendő, ha címzettje időközben meg találna halni: „Küldtem Harsányinak clavist is, ha kívántatik. Arról is instruáltam az embert, ha Harsányi meg talált halni, kivel közölje az dolgot. Rövid instructiót, az kit adtam néki, meg láthatja Kegyelmed. Pro sua prudentia Kegyelmed is instruálja. Mindenekről coram plura."[51]

A kulcsok lecserélése

Miután a kulcsmegosztás sikeresen megtörtént, és a mindkét félnél meglévő *clavis*okat beüzemelték és egy darabig használták, ideje volt elgondolkozni a lecserélésükön. Könnyű belátni, hogy egy túl sokáig használt kulcs veszélyeket rejtett magában. Minél huzamosabb ideig, minél több levélben, minél több címzett viszonylatában alkalmaztak egy adott módszert, a potenciális kódtörőnek annál több anyaga és fogódzója volt ahhoz, hogy a módszert megfejtse. Azt várnánk tehát, hogy a rejtjelezés technikájában jártas történelmi szereplők mindent megtettek, hogy ezt a veszélyt elkerüljék.

Különös, hogy míg a titkosírás-használat egyéb területeihez nagy mennyiségben találunk explicit megjegyzéseket a forrásokban, addig a kulcsok lecserélésének kérdése ritkán vetődik fel a levelekben. Mintha ez a kérdés kevéssé foglalkoztatta volna őket. És ha egyéb

[45] AR I. oszt. 2. köt. 180–181., 17. sz.

[46] AR I. oszt. 3. köt. 6–8., 7. sz.

[47] AR I. oszt. 3. köt. 673–674., 68. sz.

[48] Szilágyi Sándor (szerk.): *Kemény János és a krimiai rabok levelei 1657–1664.* MTT III/5. 609–613., 13. sz.

[49] MTT III/5. 286–290., 41. sz.

[50] MTT III/5. 292–291., 42. sz.

[51] Teleki 6. 110–112., 78. sz.

jelekből igyekszünk rekonstruálni a problémát, azzal szembesülünk, hogy a biztonság kérdését ebben a tekintetben meglepően elhanyagolták. Sem arra nem vigyáztak, hogy egy kulcsot csak egy címzett vonatkozásában alkalmazzák, sem arra, hogy a számos levélben használt kulcsot legalább évente lecseréljék.

Nézzünk erre egy példát II. Rákóczi Ferenc konstantinápolyi követeinek gyakorlatából! A követek, Pápai János és Horváth Ferenc 1706 folyamán több tucatnyi majdnem teljesen titkosított levél sifrírozásához egy olyan táblát használtak,[52] amely fontossága miatt több példányban is fennmaradt a fejedelem titkos archívumában és a Ráday levéltárban egyaránt.[53] Ha közelebbről megnézzük ezt a levélcsomagot, azt látjuk, hogy három levél majdnem azonos számkombinációval kezdődik.[54] A csomag következő levele tizenkét A4-es oldalra rúg,[55] az azt követő, gyakorlatilag teljesen titkosított levél tizenhárom oldalas.[56] Azaz, ha egy török kódfejtő történetesen kezébe kaparintotta volna a levelezést, bőséggel lett volna alapanyaga ahhoz, hogy a megfelelő elemzéseket elvégezze, és a szabályosságokat, a kódfejtéshez oly fontos ismétlődéseket is könnyen azonosíthatta volna. Pápai nem csupán akkor használta ezt a táblát, amikor a fejedelemnek írt, hanem akkor is, amikor Vay Ádám volt a levelezőpartnere.[57] A követek ragaszkodása e *clavis*hoz 1707-ben,[58] majd 1708-ban is kitartott.[59] A következő és az azutáni évben kétszer is Nándorfehérváron, majd még egyszer Konstantinápolyban találjuk Pápait, a diplomáciai környezet változása azonban nem vonta maga után a kódtábla változását, ugyanazt a *clavis*t, amit Konstantinápolyban 1706 óta használnak, alkalmazzák Nándorfehérváron 1709-ben legalább egy-két levél,[60] majd 1710-ben Nándorfehérváron és Konstantinápolyban vagy harminc levél erejéig.[61]

Meg kell adni, ez a *clavis* a szabadságharc fontosabb táblái közé tartozott. Erre nem csupán az a politikai körülmény utal, hogy a konstantinápolyi követség Rákóczi diplomáciájának kiemelt területe volt, hanem az a tény is, hogy a szabadságharcból összesen három olyan titkosírástábla maradt fenn, amelyet pergamenre (is) másoltak, és Pápai táblája ezek közül az egyik. Felirata: „Nemzetes vitézlő Pápai Jánosnak adott clavis mása."[62] A másik olyan tábla, amely pergamenen maradt fenn, Rákóczi legfontosabb diplomáciai törekvését jelzi, ez ugyanis a XIV. Lajossal és a francia udvarral való levelezését titkosította. A harmadik pedig név nélküli, nem a politikai kommunikációt szolgálta, hanem a fejedelem szerelmi ügyeit, és másutt fogunk részletesen foglalkozni vele. Bármennyire fontos szerepet játszott is a fejedelem levelezésében a tábla, mégiscsak komoly biztonsági kockázatot jelentett, hogy öt éven keresztül több város viszonylatában és több levelezőpartnerrel volt használatban. Ezek után meg sem lepődünk, hogy a száműzött fejedelem, amikor lengyelországi

[52] Mol G 15 Caps. C. Fasc 36. fol. 1-29 és Mol G 15 Caps. C. Fasc 36. fol. 1-2 - fol 80-82. Pápai követségéről lásd: Benda Kálmán: *Pápai János törökországi naplói.* Budapest, 1963.

[53] Ráday Levéltár C64-4d2-25. 12. sz., Mol G 15 Caps. C. Fasc 43.

[54] Mol G 15, A *Rákóczi*-szabadságharc levéltára, Caps. C. Fasc 36. fol. 9-10.; 11-12, 13-15.

[55] Mol G 15 Caps. C. Fasc 36. fol. 13-15.

[56] Mol G 15 Caps. C. Fasc 36. fol. 17-22.

[57] Mol G 15 Caps. C. Fasc 33. fol 35-38. Benda: *Pápai János törökországi naplói,* kiadva 9. sz. 366–367.

[58] Mol G 15 Caps. D. Fasc 80.

[59] Mol G 15 Caps. E. Fasc 109.

[60] Mol G 15 Caps. F. Fasc 160.

[61] Mol G 15 Caps. H. Fasc 226. Ebből két levél kiadva: Benda: *Pápai János törökországi naplói,* 384–389.

[62] Mol G 15 Caps. C. Fasc 43.

„bujdosásában" jellegzetes kulcsmegosztási dilemmába kerül, mert el van vágva attól a lehetőségétől, hogy olyan *clavis*t használjon, amely a címzettnél is megvan, így bizalmas információkról írjon, egyszer csak ráébred, hogy éppen Pápai tábláját újra használatba veheti Vay Ádámmal folytatott levelezésében (Gdansk, 1711. december 11): „Jóllehet mindeddig kívántam volna Kegyelmedet circumstantialiter tudósítanom: miben legyenek dolgaink? de clavis nélkül írni nem mervén, Pápai maga levele által eszemben juttatá, hogy nála lehet az régi constantinápoli clavisa, melyen íratom ezen levelemet; és mivel hűségében nem kételkedhetem, ugyan maga meg is fordíthatja."[63]

Pápai *clavis*a tehát igencsak intenzív használatnak volt kitéve. Pedig – Rákóczi utolsó, emigrációban eltöltött időszakától eltekintve – számos más titkosírástábla is rendelkezésre állt, és sok esetben erőfeszítéseket tettek arra, hogy ne ezt a módszert terheljék túl. Bay András konstantinápolyi követ 1706-ban,[64] Henter Mihály, Erdély képviseletében konstantinápolyi követ 1707-ben,[65] és szintén Konstantinápolyból Ládonyi Horváth Ferenc követ 1708-ban másik – és egymásétól is eltérő – kulcsot használ,[66] hiába vannak ugyanott, ugyanakkor, hasonló funkcióban, mint Pápai János. Maga Pápai is eltérő módszerrel sifrír-oz 1707-ben, amikor Voynovich Józsefnek ír.[67] Bizonyos helyzetekben működött a kulcsokkal kapcsolatban elvárható óvatosság, más helyzetekben a legkevésbé sem.

Az óvatlanságra jó példa Rákóczi és a bajor választó melletti ügyvivő, Vetési Kökényesdi László (az olykor Casimirius de Miloftzky álnéven folytatott) 1706–1707-es levelezése,[68] amely egy másik tábla túlterhelését dokumentálja.[69] Kökényesdi ugyanazt a *clavis*t használja Rádayval és Rákóczival magyarul,[70] mint Des Alleurs francia követ titkárával, Chamillard-ral latinul[71] és franciául,[72] sőt Kray Jakab is ezen a módszeren ír Rádaynak.[73]

A rejtjelezés fáradsága

Rákóczi Ferenc egy igen hosszúra nyúlt levelében így szabadkozik Bonnac márkinak 1708. április 25-én: „Rövidebbre fogom levelemet, hogy ne olvassa ugyanolyan unalommal, mint amilyennel titkára megfejti a clavist, tekintve, hogy látszólag apróságokról van szó."[74] A megjegyzésből két dologra következtethetünk a rejtjelhasználattal kapcsolatban. Az egyik az, hogy a sifrírozott szövegek feloldása – még a *clavis* birtokában is – fáradságos, hosszú

[63] MOL G 15. Caps. H. Fasc. 253. Egykorú másolat. Az idézett mondatot követő bekezdésekben aláhúzással jelölik a titkosítandó szövegrészeket. Kiadva: Köpeczi Béla (szerk.): *II. Rákóczi Ferenc válogatott levelei.* Budapest, 1958. 68. sz.

[64] Mol G 15 Caps. D. Fasc 81.

[65] Mol G 15 Caps. D. Fasc 80. fols. 38, 40, 46.

[66] Mol G 15 Caps. E. Fasc 109

[67] Mol G 15 Caps. D. Fasc 80. fol. 28.

[68] Ráday Levéltár C64-4d2-10. Ráday I. Pál: Külpolitikai iratok 1703–1711, Diplomáciai kapcsolatok Franciaországgal.

[69] Ráday Levéltár C64-4d2-25. (Diplomáciai levelek rejtjelezéséhez szolgáló jelkulcsok) 6. sz., másolat: MTAK, 2. sz. kiadva: Révay Zoltán: *II. Rákóczi Ferenc és korának rejtjelezése (XVIII. század).* Budapest, 1974. 65 és 76.

[70] Uo. 27. sz.

[71] Uo. 23. sz. (fogalmazvány)

[72] Uo. 24. sz. (fogalmazvány)

[73] Uo. 44. sz. Vö. Benda Kálmán et al.: *Ráday Pál iratai,* 459. 2. lj vége.

[74] Köpeczi: *Rákóczi válogatott levelei,* 39. sz.

ideig tartó tevékenység volt. A másik pedig, hogy rendszerint arra szakosodott titkárok végezték. Nézzük, mennyire állják meg a helyüket ezen állítások!

A rejtjelezett leveleket küldő és fogadó levelezőpartnerek gyakran panaszkodnak, hogy a kódolás és a dekódolás folyamata időigényes és fáradságos tevékenység. Hogy mennyire igazuk van, arról könnyen megbizonyosodhatunk, amennyiben fogunk egy átlagos, mondjuk három-négyszáz tételes homofonikus titkosírástáblát, és segítségével egy négy-öt bekezdésből álló átlagos hosszúságú levelet betűről betűre átírunk számokra. Viszonylag rövid levél esetén is igencsak elhúzódhat ez a mechanikus munka. A dekódolás pedig még több időt emészt fel, nem utolsósorban azért, mert a *clavis*ok gyakrabban sorolják a kódoló logikája szerint (a nyílt szöveg elemeinek betűrendjében) az elemeket, mint a dekódolóéban (a rejtjelszámok sorrendjében). Ez az időigényesség az oka annak, hogy takarékosabb levélírók csak egyes szavakat, mondatrészeket sifríroztak – igaz, hogy ebben az esetben pedig annak okos meghatározása volt rendkívül időigényes, hogy a levél mely részeit lehet az üzenet napvilágra kerülésének kockázata nélkül nyílt szövegnek hagyni.

Teleki Mihály 1678. július 21-án írja: „Urunk ő nagysága levelei clavissal lévén írva s estve érkezvén hozzám s jó hajnalban kelletvén megindulnom, időm nem volt az megfordításra."[75] Rákóczi Ferenc 1710. június 1-jén Munkácsról Bercsényinek: „Alig tudék az sok clavisbúl kigázolni."[76] Szintén Rákóczi 1710. március 31-én Kisérről Károlyi Sándornak: „...röviden kívánok választ adni, hogy a sok czifrázást elkerüljem."[77] Még mindig a fejedelemtől, ezúttal 1710. február 10-én, Szentmártonkátán, Bercsényinek: „Csak elhitettem magammal, hogy unalmas vólt deczifrálni Kegyelmednek az clavisos dialógusokat, az mellyeknek még extractusa is elég unalmas és bosszúságra indító materia vala előttem."[78] Bercsényi egy hónappal később, 1710. március 10-én a dekódoláshoz szükséges alkalmas időt hiányolja: „Levelemet elvégezvén, érkezett egy böcsületes kapitányember, a ki az Felséges Fejedelemnek elhozta az aranybárányt, hozván magával hosszas clavisált leveleket, mellyeknek megfordításában alkalmas idő múlik, s úgy is, minthogy franczia nyelven vannak, a kibűl keveset tanúlhatok, tovább ezen levelemet tartóztatnom nem kívántam."[79] Kemény Simon 1662. május 27-én Aranyos-Medgyesen így kéri Teleki Mihályt: „Adjon Isten minden jókat Kegyelmednek. Háromrendbeli leveleit is vettem Kegyelmednek. Az Istenért kérem Kegyelmedet, az dolgot, az mi oly szükséges, írja meg breviter, ne írjon ilyen rettenetes nagy pandechtákat, még penig czifrával s igen hibásan, mert az követ úr itt lévén, annyi az dolog, hogy étszakánk sincsen."[80] Udvarhelyi György 1664. szeptember 2-én Teleki számára más, sifrírozott levelek tartalmát foglalja össze. E levél végén írja: „...az éjszaka az clavissin munkálódtam."[81] Thököly így ír naplójában 1693 márciusában: „Az éczakának is nagy ríszit az levelek olvasásában töltöttem, megfordítván az clávisos írásokat is az éjjel, és az levelek revideálásában is végetérvén, hivattam az franczia urat."[82] A desifrírozás tehát nem ritkán követelt éjszakázást.

[75] Teleki 8. 228–229., 195. sz.

[76] AR I. oszt. 3. köt. 113–114., 72. sz.

[77] AR I. oszt. 3. köt. 85–86., 51. sz.

[78] AR I. oszt. 3. köt. 19–20., 14. sz.

[79] AR I. oszt. 8. köt. 208–209., 32. sz.

[80] Teleki 2. 271–272., 201. sz.

[81] Teleki 3. 227–229., 181. sz.

[82] Nagy Iván (szerk.): *Késmárki Thököly Imre naplója, 1693–1694.* Monumenta Hungariae Historica 2. Scriptores 15. Pest, 1863. 43.

A rejtjelező személye

Teleki Mihály 1678. március 6-án Naláczi Istvánnak írt levele arról árulkodik, hogy a kódfejtés specialistát igényelt: „Itt írhatnék többet is, de bánnám nehézséget vennék ő nagyságától. Ha tudnám, kivel fordíttatja meg, clavissal megírnám, mert szükség volna Kegyelmednek tudni."[83] Ugyanerre utal Esterházy Dániel 1711. február 13-án kelt levele Rákóczinak: „...hogy penig magam nem írhattam saját kezemmel, alázatossan bocsánatot várok Fölségedtül, tizenegy naptul fogva való ujjabb súlyos nyavalyám okozta, de mely emberem ezt írta és ki minden titkos communicatiómat folytattya, igaz magyar, igen [bízom] benne, mind magamban, nem kételkedem, mert régen ismerem, azért adhibeálom bátran minden titkaimban."[84]

Időnként név szerint azonosítható az ember, aki – ahogy a szövegek mondják – „megfordítja" a *clavis*t („az clavis kezemben jött, meg is fordítottam" – írja Kende Gábor).[85] A fent említett Naláczi István bizonyos Baló úrra hivatkozik 1668. május 16-án Gyulafehérvárról küldött levelében: „Clavissal is írt Székely Mózes urunknak, de még Baló uram nem érkezék be, hogy megfordítsa; meg lévén, Kegyelmedet tudósítom."[86] Bay Mihály írja diáriumában: „...az leveleket néki praesentáltuk, és minthogy igen rövid volt az idő, az urunk levelét, minthogy clavissal volt némelly része, meg nem olvashatta, hanem adta Bukken uramnak, hogy leczifrázza."[87] II. Rákóczi Ferenc 1711. március 14-én Sztaro-Zelóból ekként inti Sennyei Istvánt: „...az clavisatiót, a mennyire erőtlensége engedi, maga vigye véghez, ha penig nem, Körösy György komornikra bízhatja."[88] Bercsényi Miklós 1706. október 2-án Tornáról a fejedelemnek címzett levelében a titkos jegyek felfejtőjére, bizonyos Jánoki úrra hivatkozik. Jánoki, ha jól értjük a levelet, nem csupán a *clavis* birtokában dekódoló titkár, hanem ellenséges kódok feltörésének is szakembere volt: „Ezelőtt egy órával érkezének Gyöngyösről egy ráczkevi magyar emberrel, kit ezen levelekkel Budárúl küldtek volna az német táborra; Miskolcznál mondta az Generális, hogy előltanálja. Az, magyarságától viseltetve, ingyenessen gyütt Gyöngyösre, s idehozták; megküldtem, Kegyelmes Uram, Nagyságodnak, – múlassa magát Jánoki Uram, mert én semmit sem tudok benne."[89]

A források tehát arra utalnak, hogy a kódok felfejtését arra specializálódott titkárra, komornyikra, szakemberre bízták. Ez így is logikus, nagy fontosságú politikustól nem várhatjuk, hogy a harcmezőn felállított sátrában, a fejedelmi udvarában vagy a diplomáciai taktikázások közepette maga pazarolja az idejét egy ennyire mechanikus és hosszan tartó tevékenységre. Annál inkább meglepődünk, amikor arról értesülünk, hogy Thököly Imre vagy II. Rákóczi Ferenc mégiscsak rendszeresen pazarolták.

Thököly fent idézett megjegyzése arról, hogy a *clavis*okat éjjel fordította meg, ahogy arra az alábbi megjegyzés is egyértelműen utal, maga végezte ezt a tevékenységet: „Az leveleket percurrálván és az clavisosokat is megfordítatván, azután hivattam a franczia urat is, ki

[83] Teleki 8. 96–97., 88. sz.

[84] MOL G 15. Caps. H. Fasc. 237. Kiadva: Bánkúti Imre: *Források Kassa 1710–1711. évi védelméhez.* Hadtörténelmi Közlemények, 116. évf. (2003) 3-4. sz. 856–932., az idézett levél: 910–911., 17. sz.

[85] Teleki 4. 448–449., 328. sz., 1669. április 2.

[86] Teleki 4. 296–297., 220. sz.

[87] Thaly Kálmán (szerk.): *Késmárki Thököly Imre és némely főbb hívének naplói és emlékezetes írásai, 1686–1705.* Pest, 1868. – Második rész. Tököly Imre némely főbb híveinek naplói, írási, 1686–1699 (Monumenta Hungariae Historica 2. Scriptores 23), 547.

[88] AR I. oszt. 3. köt. 602., 22. sz.

[89] AR I. oszt. 5. köt. 280–283., 141. sz., idézet: 282.

ebíden is nálam volt."[90] Később: „Érkezék meg a lengyel postám Drinápulybúl, nagy pachetákbúl álló levelekkel, kiknek revideálásában töltöttem el az egész napot, de mégsem érhettem véget benne, minthogy sok clavisos írások vadnak benne."[91] *Clavis*okról, clavizálásról nagyon gyakran tesz említést a naplójában, láthatóan mindennapi gondolatainak részét képezte a rejtjelezés, és másutt is említi naplójában, hogy a *clavis*ok megfordítását maga végezte.[92]

Bár a Rákóczi-szabadságharc rendkívül kiterjedt levelezését és annak sifrírozását nagyrészt a fejedelem megbízható titkárai, Ráday Pál, Pápai János, Krucsay István, Beniczky Gáspár végezték, Rákóczi fent idézett levelei („Alig tudék az sok clavisbúl kigázolni," „a sok czifrázást elkerüljem") egyértelműen arra utalnak, hogy a rejtjelezést azért tartja fáradságosnak, mert maga is gyakran végzi. Megerősít ebben Beniczky Gáspár naplója: „Ő felsége az posta vétele után szobájába visszavonulván, magánosan clavisos levelek megfejtésében derekasan munkálkodott."[93]

Elővigyázatosság és elbizakodottság

A források számos közvetlen és közvetett információt tartalmaznak arra nézve, mennyire voltak a rejtjelezők tisztában a sifrírozott tartalomra leselkedő veszéllyel, mennyire igyekeztek megóvni a titkosírásukat a lelepleződéstől, mennyire tették ellenállóvá, mennyire számítottak kódtörők támadására. A forrásokból kinyert információ azonban rendkívül ellentmondásos, legalább annyi jel utal arra, hogy körültekintőek és óvatosak voltak, mint arra, hogy a leghalványabb elképzelésük sem volt, mivel teszik kiszolgáltatottá titkosírásaikat.

Nézzük előbb, mi utal az óvatosságra! A titkosírástáblák tételes vizsgálata során megállapíthatjuk, hogy számos tábla külön kódjelet rendelt a számoknak és a hónapneveknek.[94] Ez azért bölcs eljárás, mert dátumozás szinte minden levélben előfordul, ráadásul kitüntetett helyen (a levél elején vagy a végén), és ha a kódfejtő több levél birtokába kerül, a betűnként sifrírozott dátumozásban rejlő szabályosságokat kiismerve könnyen betörési pontot találhat a rendszerbe. Amennyiben bekalkulálja a forgalomanalízisből származó információkat is, azaz, hogy melyik levelet melyik hónapban adták fel, megbízható fogódzót kaphat a hónapok azonosításához. Ha azonban a hónapnevek nem betűnként kódoltatnak, hanem egy hónapnév egy számot kap, úgy azt hiába azonosítja helyesen a kódtörő, ezáltal nem nyer betörési pontot az ábécé rejtjelezésébe. Ugyanez a helyzet a megszólításokkal és a címzett nevével, amelyek (a forgalomanalízis révén) szintén a könnyen azonosítható elemek közé tartoznak: az, hogy ezek külön számot kapnak a táblákban, a tervező bölcs óvatosságáról árulkodik. Hasonló tudatosságra utal az az eljárás, amikor a számok a táblázatban nem a nomenklator táblázat betűrendjében „követik" egymást (azaz a kódszámok sorrendje és a kódolandó szavak betűrendje nem felel meg egymásnak), hanem vízszintesen vannak elhelyezve. Így a dekódoló ugyanolyan kényelmesen megtalálja őket, a kódfejtőnek azonban nem jelentenek olyan praktikus fogódzót a kódjelek azonosításában, mint amikor az azonos betűvel kezdődő szavak egymáshoz közeli számokat kapnak.

[90] Nagy: *Késmárki Thököly Imre naplója*, 64., hasonló idézet: uo. 33.

[91] Nagy: *Késmárki Thököly Imre naplója*, 298.

[92] Nagy: *Késmárki Thököly Imre naplója*, 299.

[93] Idézi: Révay: *II. Rákóczi Ferenc rejtjelezése*, 60.

[94] Például a Mol G 15 Caps. C. Fasc 43-ban.

Ehhez hasonló felismerés munkálkodhatott Teleki Mihályban, amikor Apafi Mihálynak küldött levelét teljes mértékben titkosította, a keltezést azonban meghagyta nyílt szövegnek.[95] Miért is rejtjelezné a dátumot és az aláírást, amikor a potenciális kódfejtő úgy is tisztában van azzal, ki, honnan és mikor küldte a levelet, nem jelent veszélyt megadni számára az amúgy is ismert információkat. Azonban érdemes elkerülni, hogy olyan rejtjelezett szövegrészt kínáljunk neki, amelynek a levél keletkezését ismerve ki tudja találni a tartalmát, mert akkor megnyílik az út az egyes rejtjelek azonosításához. Paradox módon tehát, és ez az, amit Teleki felismert, egyes információk nyíltan hagyása növelheti a titkosított információ biztonságát.

Efféle közvetett utalásokból rekonstruálhatjuk, mennyire tisztában voltak a veszéllyel, de óvatosságuk természetesen explicit megjegyzésekből is látszik. A rejtjelkulcsot és a rejtjelekkel írt leveleket védeni igyekeztek. Bánffy Dénes Telekit kérdezi 1660. augusztus 30-án, kiadhatja-e másnak *clavis*át: „Én ez óráig Kegyelmednek egy czéduláját sem láttam, noha értettem volt, hogy Kegyelmed küldött, de azt Barcsai Gáspár uram intercipiálta és oda van; kérette az clavissát tűlem, de nem adtam, nem tudván Kegyelmed mikről írt volt benne. Kegyelmed azért tudósítson, mik voltak bele írva, mert suspicálódnak valóban érette."[96] Ugyanő ugyanannak 1662. december 19-én egy gazdagon titkosított levélben megjegyzi, hogy Ébeni István kapitányt arra kérte, a nála lévő leveleket biztonsági okokból égesse el.[97] Két héttel később még egyszer ugyanaz a levélíró és címzett, sőt a levélben említett személy is, a téma pedig a levélinformáció sérülékenysége: „Kérem, levelemet Ébeni uramnak elég securitással küldje el; bánnám vagy német, vagy más idegen kézben akadna, mert ezekről az dolgokról bővön írtam s nem is mindenütt clavissal."[98]

Amilyen gazdag az óvatosságra utaló megjegyzések száma, legalább annyi jel utal hanyagságra és logikátlanságra is. Nézzünk egy példát az utóbbira ismét csak a titkosírástáblák köréből. Szepesi Pál *clavis*ában hiába sok a *nullitas (errantes seu nihil significantes)*, és hiába van a magánhangzóknak négy-négy kódjele is, kódszavak és szótagjelek híján, valamint a betűk többségének csupán egy jelet rendelve mégiscsak gyenge és sérülékeny rendszert épített a tervezője (nem is beszélve arról, hogy a 17. század végén grafikus jeleket keverni a számokból álló titkosírásba nem vall a kor követelményeinek a felismerésére).[99]

Különös hanyagságra bukkanunk akkor is, ha egyes leveleket olvasunk el figyelmesen. Absolon Dánielre általában jellemző, hogy gyakran, de takarékosan clavizál, azaz sok levélben keveset titkosít. Igyekszik bölcsen megválasztani, melyek azok a szövegrészek, amelyeket el kell rejtenie a kíváncsi olvasó elől. Ez önmagában lehet jó döntés, az alábbi, 1678-as levélkezdetben azonban nem tűnik annak: „Kegyelmed 12. praesentis Kővárban költ levelét alázatosan vettem, a *pirongatást szivemnek* kiírhatlan *szomorúságával* megértettem. Ha mentségre fakadni akarnék, sok szóból állana a levél. Szükséges mindazonáltal rövideden megfelelnem, az *elkeseredett lélek* nem is engedi, hogy hosszas legyek." Ha mármost mi vagyunk az illetéktelen olvasók, és az eredeti levelet kaparintjuk meg, amelyben a dőlttel szedett szavak titkosítva vannak, azaz helyükön csupán számokat látunk, vajon mit érte-

[95] Teleki 8. 240–241., 212. sz.

[96] Teleki 1. 555–556., 475. sz.

[97] Teleki 2. 398–399., 295. sz.

[98] Teleki 2. 412–415., 304. sz. 1663. január 2.

[99] ÖStA HHStA Ungarische Akten Specialia Verschwörerakten VII. Varia (Pressburger Kommission etc.) Fasc. 327. Konv. D. Chiffres 1664–1668, fol 3.

nénk belőle? Próbáljuk e szavak nélkül újraolvasni a mondatokat! Nehéz lenne azt állítani, hogy értékes információt vesztenénk.[100]

Ugyanebből a levélből nézzük az alábbi bekezdést: „Hogy *fogyatkozások* és sok kiváltképpen való akadályok voltak erről a részről, Kegyelmednek megirtam; specificatióra menni nem ítéltem jónak, sem szükségesnek, hanem inkább a mely *fogyatkozások* voltak is, reparálni s elhárítani igyekeztem; contra rationem status et interesse publicum gondolván lenni holmi reparalandó *defectusokkal* az elméket elirtóztatni; építeni, nem rontani kívántam." Következetesen rejtjelezi a „fogyatkozások" és „defectusok" szavakat, de a mondatszerkezetből is láthatóan szinonim „kiváltképpen való akadályok"-at nem titkosítja. Úgy tűnik, Absalonnak ebben az esetben nehezére esett, hogy a potenciális ellenfél fejével gondolkodjék.[101]

A következő évben hasonló következetlenségről tesznek tanúbizonyságot a Telekinek író bujdosók. Rájuk egyébként is jellemző, hogy leveleiknek csupán kis részét titkosítják, ebben a levelükben azonban csak három szót: „Dévény és Torna *körül levő hódolt* helyeket is csak elpusztított." Mit lát ebből az ellenség? „Dévény és Torna xxxx xxxx xxxx helyeket is csak elpusztított." Bizonyos mennyiségű információt persze elveszt a *clavis* birtokában lévő hivatalos címzetthez képest, de igazán nem sokat, és amennyiben ismeri a bekövetkezett harci eseményeket, úgy valószínűleg pontosan tudja, mely helyekre gondolt a levélíró.[102]

Már említettük, hogy Pápai János, aki a csak részben baráti porta fővárosában volt követ, veszélyesen sokáig nem váltotta Rákóczinak küldött leveleinek kulcsát. Márpedig levelet nagy mennyiségben írt a fejedelemnek, és ezeket gazdagon sifrírozta. A legkevésbé sem volna meglepő, ha a törökök megállították és lemásolták volna leveleit. Márpedig, ha gondosan összehasonlították volna három egymást követő levelét, amelyekről mi ma a megfejtés birtokában tudjuk, hogy a „Kegyelmes Uram" megszólítással kezdődnek, bizonyára ők is felismerték volna, hogy a levélkezdő számkombinációk majdnem teljesen megegyeznek, és bizonyára azt sem esett volna nehezükre kitalálni, vajon mit jelenthetnek.

Ke. gy. el. me. s. Ur. am.
133. 39. 32. 273. 80. 205. 61[103]

Ke. gy. el. me. s. Ur. am.
133. 39. 364. 32. 273. 308. 205. 61[104]

Ke. gy. el. me. s. Ur. am.
133. 39. 32. 273. 80. 205. 61[105]

Ke. gy. el. me. s. Ur. am.
133. 39. 32. 273. 80. 205. 61[106]

[100] Teleki 8. 179–186. 154. sz., ugyanez: MTT III/6. 6-13., 1678. ápr. 28.
[101] Uo.
[102] Teleki 8. 428–429., 408. sz.
[103] Mol G 15 Caps. C. Fasc 36. fol. 3-4
[104] Mol G 15 Caps. C. Fasc 36. fol. 9-10
[105] Mol G 15 Caps. C. Fasc 36. fol. 11-12
[106] MOL G 15 Caps. C. Fasc 36. fol. 13-15.

Ennek márpedig – ismételjük – nem az a veszélye, hogy megtudják, a levél a fejedelemnek szólt, mert ezt nyilván korábban is tudták, hanem az, hogy a feltört szövegrész segítségével a siker reményében támadhatják meg a rejtjelszöveg többi, értékesebb és bizalmasabb részét.

Ugyanez a veszély jelentkezik, ha valaki gondosan összehasonlítja Rákóczi lengyel levelezőpartnereivel folytatott gazdag korrespondenciájának egyes leveleit.[107] A Magyar Országos Levéltárban őrzött G 15. Caps. C Fasc. 39 összesen kétszáztizennégy foliónyi anyaga körülbelül száz titkosított és tizenöt nyílt, francia nyelvű levelet tartalmaz 1704–1706-ból. A levelek titkosítása ismét a francia követekkel használt táblák szerint történt – ezek a maguk négyszázötven kódjelével a szabadságharc legkidolgozottabb táblái közé tartoztak.[108] Hiába azonban a fejlett módszer, a levelek közül ugyanis negyven kezdődik majdnem azonos módon, az „a Danzik, le 20 Février, Monsieur" rejtjelezett formájával (amelyben természetesen a dátum változik). Az egyes számkombinációk – homofonikus kulcs lévén – eltérnek ugyan, az anyag azonban kellően gazdag ahhoz, hogy egy ellenséges ügynök figyelmes vizsgálattal az egymásnak megfelelő szótagokat és betűket jelentő számokat helyesen azonosítsa.[109] Még a nullitások, a semmit sem jelentő kódjelek sem fogják nagyon zavarni, azokat ugyanis a levélíró majdnem mindig a sor végére szúrta be. Ilyen hanyag használat mellett hiába homofonikus a rendszer, és hiába rejti Rákóczi magát Nathanaél Sylver vagy Pompeio Cesoni álnevek mögé, üzenetei könnyen lelepleződnek.

Amikor a technika csikorog

Egy olyan technológia alkalmazásába, amelyet sokan sokféle célra használnak (ráadásul olykor nehéz körülmények közt), gyakran csúszik hiba. Nincs ez másként a rejtjelezéssel sem, a történelmi szereplők sokszor szembesültek nehézségekkel, olykor egészen mulatságos körülmények közt.

A leggyakoribb és legprózaibb probléma a rejtjelezett levélnek megfelelő titkosíráskulcs hiánya volt. Bethlen Miklós Teleki kérésére, hogy Harsányi Jakabnak válaszoljon, szabadkozik, hogy annak levelét nem tudja elolvasni: „Úgy látom, Harsányi az maga nevét is clavissal írta, annak az mása kinél lehet?"[110] Bánffy Dénes hasonló helyzetben komoly erőfeszítéseket tesz, hogy megtalálja a kulcsot: „Incéditűl is érkezék levél Caneábúl. Írja, már közel lévén az vezérhez, de clavissal lévén írva levele, máig is fordítás nélkül van, mert se Bethlen János és Miklós uraméknál nincs az clavis párja; most Balóhoz vitték, ha ott lenne az clavis."[111] Szepesi Pál pedig Teleki levelének kulcsát keresi hasonló buzgalommal: „Kegyelmed clavissal írt levelei jöttek, Uram, kezemhez, de boldogúl elő nem mehettem bennek, mivel az mely clavissal Kegyelmed írt, se Keczer, se Vér Mihály uramék sem adák sem küldék meg és így ma is vak vagyok sok terminusokban." Levele végén még egyszer emlékezteti Telekit: „Az Kegyelmed csinálta clavist, kérem, küldje meg."[112] Maga Teleki pár évvel később Thököly Imrén egyszerre két levél *clavis*át is keresi: „Udvarhelyi, [...] amit nekem írt volt, azt nem tudtam elolvasni, azért izentem Forval uramtúl a clavisnak idekül-

[107] Rákóczi lengyel kapcsolataihoz lásd: Iványi Emma: *II. Rákóczi Ferenc politikai levéltára, 1526–1712.* Levéltári Közlemények, 25. évf. (1954) 1. sz. 130–140., különösen: 133–134.

[108] MOL G 15 Caps. C. Fasc 44.

[109] MOL G 15. Caps. C Fasc 39.

[110] 1671. október 22. Teleki 5. 625–627., 425. sz.

[111] 1668. március 1. Teleki 4. 278–279., 206. sz.

[112] 1672. november 5. Teleki 6. 394–398. 264. sz.

dése felől. A másik clavis micsoda clavis, örömest érteném."[113] Néhány évvel később Bethlen Gergely Teleki levelét nem érti: „Kegyelmed levelét is én bontottam fel, de semmi hasznát nem vehettem, mert clavissát nem tudom."[114] Rájárt a rúd a *clavis*okra ezekben a napokban, Thököly Imre két nappal később írja Telekinek: „Ubrisi uram clavissát elvesztvén, látja Isten, mit tegyen 88, nem tudhatom."[115]

A probléma – tudniillik a *clavis* hiánya – meglehetősen tartósnak bizonyult Teleki 1666. július 6-i, Széchy Máriának írott levelének esetében.[116] A számokkal teli levélre Széchy három héten belül válaszolja saját levele végén, külön papíron: „Édes Teleki Uram, az Kegyelmed kis levelére választ nem adhattam, az clavisát nem küldte meg, hanem kérem szeretettel, küldje meg."[117] A *clavis* azóta sincs meg, ez Teleki azon levelei közé tartozik, melyeket még nem tudunk dekódolni.

Más nőknek is meggyűlt a bajuk Teleki *clavis*aival. Húga, Bornemissza Kata kérdezi őt: „Édes Öcsém uram, az mely levelet Kegyelmed most az postától küldött, én nem tudtam mind el olvasni, mivel nincsen nálam leírva abban az írásban, az kit Kegyelmed itt hagyott. Ezek azok az kiket nem tudtam: 020, 550207, 4y04, 9100, ezek nincsenek nálam."[118]

Bethlen Miklós 1667. április 7-i levelét érdemes hosszabban idézni. A kiindulási helyzet a szokásos, beszámol egy levélről, amely *clavis*ának nincs birtokában. Azonban a levél nem számokkal van sifrírozva, hanem – a magyar történelem más szakaszaiból is ismert módon – a kulcsfontosságú szavak helyett állnak más jelentésű szavak. Így a végeredmény értelmesnek, de érdektelennek tűnő magyar szöveg, de a kulcs birtokában, azonosítva, mely politikai és földrajzi nevek vannak kicserélve, bárki könnyen felfejtheti igazi jelentését. Bethlen mindenesetre hosszan idézi a levelet, majd maga próbál értelmet adni neki: „Bory levelét én alig értem. Írja: Palatinus életéhez már semmi reménség nem volt, s ha meghal, elég nagy változás ugyan, de ezzel nem csorbul meg Istennek ő szent felségének nagy ereje. Az Moldovából és Havasalföldéből való kereskedés hogy megindulhasson, nem itélem hasznosnak s úgy is reménlem, nem leszen annak futamottja. Azonban csak lássuk már, mire fordul az szegény úr dolga. Ha soha onnét csak egy lovász alá való paripát nem hoznak is, nem hinné Kegyelmed, itt is az jó gazda emberek minemű szép méneseket nevelnek. Más az, nem tudom, értette-e Kegyelmed, Bécsből is már megindult a kereskedés egész Konstantinápolyig, az kinek kedve s pénze leszen, ezen commoditassal mind lovat, mindent kihozhatni. – Ezek az Bory szavai, melyeket én nem értek, mert olyan clavisom vele nincsen. Az moldovai s havasalföldi kereskedésen, úgy hiszem, érti az török segítségét, mely neki nem tetszik s bizony nekem sem tetszett soha s nem is tetszik; az míg én oda ki voltam, akkor úgy nem gondolkoztak volt. Bécsi kereskedésen érti, gondolom, az Franczuz állapotját, talám annyira, hogy ha mü emberek nem lennénk neki, az Franczuz által is traktálhatnának. De ez csak vélekedés s bizonyosan mit értsen rajta, nem tudhatom. De az akarmint legyen, az clavissal írt resolutiojok szerént Baló után írunk ezen mai nap."[119] (Érdemes felfigyelni arra, hogy a levél végén említett Baló úr több levélben is feltűnik mint a *clavis*ok szakértője.)

[113] 1677. szeptember 25. Teleki 7. 512–513., 355. sz.
[114] 1679. január 29. Teleki 8. 400., 376. sz.
[115] 1679. január 31. Teleki 8. 401–402., 378. sz.
[116] Teleki 3. 582–583., 432. sz.
[117] 1666. július 26. Teleki 3. 592–593., 441. sz.
[118] 1658. július 6. Teleki 1. 220–221., 191. sz.
[119] Teleki 4. 78–80., 63. sz.

Más esetekben nem az okozza a problémát, hogy a címzettnek nincsen *clavis*a, hanem az, hogy vagy a levélíró nem tudja, melyiket használhatja a kódoláshoz, vagy pedig a címzett nem tudja, melyiket kéne használnia a dekódoláshoz. Thököly Imre 1679. október 29-i leveléből szépen kirajzolódik, hogy a bújdosó fejedelem mennyire tisztában volt a titkosírások biztonságos kezelésének részleteivel: „Az clavis dolgában nem tudok Uram eligazodni, mert én két rendbéli clavissal is írtam Kegyelmednek s nem tudom, melyiket érti. Az mely clavisom azért Kegyelmeddel volt, azt egészen elhagyom s elszaggatom; ezen levelemet pedig Faigel uram clavissával írtam. Nem is lesz vala bátorságos az clavisos levelet clavissal együtt elküldeni; Kegyelmed csináltasson újjobbat, éljünk azután avval."[120]

Bethlen Miklós 1667. augusztus 23-án írja, hogy több próbálkozással sem tudta a megfelelő *clavis*t azonosítani: „Bocskai uram ez inclusát küldte ide. Próbálván nyolcz vagy kilencz clavissal, el nem tudám olvasni. Küldje vissza Kegyelmed Gyulafi uramtól, maga talám meg tudja fejtetni; vagy talám amaz nagy régi clavissal van irva, melynek párja én nállam nincsen."[121]

Pápai Gáspár 1706-os, Rákóczinak küldött levelében egészen nehéz követni az egyes *clavis*ok útját: „Vajnovics uramnak Nagyságod méltóságos levelét megadtam, de az includált czifrák nem consonalvan, semmit az Nagyságod levelében el olvasni nem tudott és még mióta Nagyságodtul el jött, vette ugyan két rendbéli leveleit Nagyságodnak, de egyikének sem tudhatta magyarázattyát s értelmét, kihez képest mind az oda küldött czifrát s mind az Nagyságod levelét vissza küldötte, meg hagyván magánál az czifrának párját, hogy ezután azon czifrákkal írasson Nagyságod és el ne változtassák, mint most esett feledékenységből, az maga levelét penig most Nagyságodhoz az én czifrámmal írta."[122]

Hasonlóan bizonytalanodik el a fejedelem, amikor nem találja a megfelelő kulcsot. Maga Rákóczi írja Ráday Pálnak 1709. december 5-én Munkácsról: „Az Kegyelmednek elmenetelétűl fogvást Moldvábúl többet egy levelénél nem vettük, melyben ámbár kevés legyen is, annak megfordítását véghez nem vihettük, ámbár azon clavissal is próbáltuk, a mellyet Landor-Fejérvárra menetelekor Pápainak adtunk vala. Melyre nézve kíntelenítettük az Károlyi úr clavisával élni, az mellyet Kegyelmed memoriter is tudhat, s egyszer már Eszterház Dánielnek is hasonlót adtunk vala."[123] Tíz nappal később Rákóczi visszatér az esetre, ezúttal már a megoldás birtokában: „Noha a minap, Munkácson létünkben, vévén az Kegyelmed 3-9-bris datált levelét, sokféle clavisokkal próbálgatván, meg nem fordíthattuk vala, és ugyanazért kíntelenítettük Károlyi úr clavissával élni, vévén mindazonáltal tegnapelőtt 21. írott levelét is: annak megfordításában nagy-nehezen reáakadtunk a clavisra, a mint is ezen levelünket avval írjuk, és azután is bízvást élhet Kegyelmed véle."[124] Szélsőséges esetre tűnik utalni az a megjegyzés, amely szerint Rákóczi egyszer azt sem tudta eldönteni, néhány „előtte suspectus" levél „clavisos-é vagy csak lengyel".[125]

Rendszeresen előfordul, hogy a címzett – kisebb vagy nagyobb szemrehányással – visszajelez, hogy nem képes a rejtjelezett szöveget elolvasni. Pataki Mihály Nemes Jánosnak írja 1678. január 23-án: „Kegyelmed clavissának én bizony nagyobb részét el nem tudtam

[120] Teleki 8. 543–547., 526. sz.

[121] Teleki 4. 176–178., 134. sz.

[122] Benda Kálmán et al.: *Ráday Pál iratai: 1703–1706*. 1. köt. Budapest, 1955. 728.

[123] AR I. oszt. 2. köt. 582–583., 125. sz.

[124] 1709. december 15. (a szövegkiadásban valószínűleg tévedésből: december 5.) AR I. oszt. 2. köt. 591–594., 135. sz.

[125] AR I. oszt. 3. köt. 75–78., 46. sz.

olvasni."[126] Wesselényi Pál 1678. október 29-én: „Szepesi uram igen vétkesen írta a clavist, kivált Szalai uram felől való dolgot semmiképpen nem érthetem, úgy az Kgd írta cédulának is a végit; a többit kitanáltam."[127] Pár nap múlva megismétli: „Én Uram az Szepesi uram írta clavisos írást annyira nem értettem."[128] Maga Szepesi Pál is hasonló helyzetbe kerül Telekivel szemben, ugyanis visszakérdez: „Azt az nagy D-t Kegyelmed levelében, és az [itt megismétli a grafikus jelet] soha ki nem találhatom, noha én azt is jóra magyarázom."[129] Bánffy Dénes 1670. március 27-én Telekinek: „Micsoda arany felől ír postscriptában, hogy szép dolgok vannak oda ki felőle, én bizony Kegyelmed írását nem penetrálhatám. Bár nekem ne írna ilyenkor clavissal!"[130] Naláczi István és Székely László még kevésbé kíméli Telekit, levelükben humor keveredik a szemrehányással: „Az Kegyelmed boszorkány írása, kit rettenetes főtörődéssel kell nekünk olvasnunk. Sok dolgokrúl írván kegyelmed, egyiket míg kisillabizáljuk, a másikat elfelejtjük. Kezdeti ugyan még is van, de a végére mintha kűvárvidéki bikákat bocsátottak volna mászkálni."[131] Nem nélkülözi a szemrehányást Bethlen Miklós Telekinek írt levele sem: „Az Kegyelmed levelét az palatinusné soha el nem tudá olvasni, én sem tudám, s ha ezentúl úgy írnál is, nem tudnám, ha ugyan tizenkét oculárt tennék is az orromra; igazán bizony czifrával volt, talán bizony magad sem tudtad volna elolvasni; másszor nem árt rendesebben írni, mert egy szóval nem tudja senki jól, mi vagyon benne."[132] És ha visszaugrunk az időben egy pár évtizedet, Kászonyi pátert idézhetjük, aki I. Rákóczi György írásáról így emlékezik: „Szegény Rákóczi György fejedelemtől hallottam, – valakinek két-három levelére egymás után választ nem teszen, ne is próbálja többször, mert unalmas előtte annak írása. Már pedig az ő ákom-bákumait betűzgetni nem lehetett nagy gyönyörűség; sokszor el sem lehetett olvasni. Nem tudok a cziffrán eligazodni, mit parancsoljon Kegyelmed, hogy vegyek: késeket, kecskéket, avagy kecsegéket."[133]

Előfordul, hogy a *clavis* rendelkezésre állt, de hibás volt, vagy hibásan alkalmazták. Absolon Dániel egy levelében egyszerűen eltéveszti a nomenklator számokat, és a szövegben 241-et, azaz lengyel királyt ír 240, azaz francia király helyett.[134] Mulatságos, hogy két hét múlva egy másik levelében (talán a kárpótlás céljával) éppen fordítva követi el ugyanezt a hibát, és francia királyt ír lengyel helyett: „Nem tudom, ha a *magyar nemzet* most és jövendőben ellehet-é a *francziai* és *franczia királyok* nélkül."[135]

Sokszor a levelezőpartnerek tesznek szemrehányást. II. Rákóczi György írja Balogh Mátyásnak egy nappal 1657 karácsonya előtt: „Elvettük 3. írt kegyelmed levelét, az clavist nem olvashatjuk, mivel vétkes, nem is érthetjük jól a dolgot."[136] Rhédey Ferenc rejtjelezési hibákat mutat ki levelezőpartnere titkosítási módszerében: „Ha oly dolog interveniál, és alkalmatossága leszen Kegyelmednek, hogy nekem írjon, az clavist igazabban írja, mert némely

[126] Teleki 8. 39–40., 37. sz.

[127] Teleki 8. 310–312., 288. sz. (C.Wes.07)

[128] 1678. november 8. Teleki 8. 323–325., 301. sz.

[129] 1676. január 24. Teleki 7. 158–159., 118. sz.

[130] Teleki 5. 126–127., 79. sz.

[131] 1676. január 14. Teleki 7. 140–142., 104. sz.

[132] 1666. július 27. Teleki 3. 594–596., 442. sz.

[133] Idézi Révay: *II Rákóczi Ferenc*, 76

[134] 1678. április 29. Teleki 8. 188–191., 157. sz.

[135] 1678. május 16. Teleki 8. 195–198., 162. sz.

[136] Szilágyi Sándor (szerk.): *Monumenta Hungariae Historica 4. Diplomataria. 23.: II. Rákóczi György diplomacziai összeköttetéseihez.* Budapest, 1874. – 1657, 589.

betűk meg sem ismerszenek, úgy írja Kegyelmed; némelyikének pedig kettőnek is vagyon egy signuma, azt is valamivel variálja Kegyelmed."[137]

Thököly azonosítja követe, Bay Mihály egy clavizálási hibáját: „Írta kegyelmed azomba a Csáffer passa postája által irt leveliben clavissal: az francziai orator mint volt szembe a letett vezérrel, és a mi személyünk s accomodatiónk iránt micsoda oblatiókra fokadott; de talám a clavisban kegyelmed errálhatott, mert az orator a Brassai által küldött leveliben a tatár chámmal lött conferentiájárul emlékezik, – kirül való világosítását is kegyelmednek elvárjuk."[138]

A háromszáz év előtt élt emberek finom humorát azonosíthatjuk az alábbi esetben. Rákóczi egy Pápai Jánosnak Miskolcról írt levelében abban kéri követe közreműködését, hogy Szeged megszállásához kérje a porta beleegyezését.[139] Azonban Szeged nevének kódolását elronthatta a fejedelmi kancellária, ezen viccelődik 1706. május 16-i, természetesen kódolt válaszlevelében Pápai, aki persze az elrontott *clavis* ellenére is jól tudta, melyik városról van szó: „Parancsollya Nagyságod, impetrállyuk, hogy a [...] vezér engedgye meg Nagyságodnak Szrülavárnak megszállását. Eléggé voltunk curiosusok benne, hogy azon helyet az mappában feltalálhassuk, de oly erősséget nem találtunk, s nem is tudunk az magyar corona alatt, nem lehet munkában is vennünk. Hogy ha penig Nagyságod Szeged várának megszállására kíván szabadságot, az midőn még Nagyságod protectiója alatt nincs, az töröknek nem láttuk szükségesnek, hogy erre engedelmét kérjük..."[140]

Néha nem világos, ki is hibázik (többet) a levelezőpartnerek közül, ilyenkor lehet kölcsönösen szemrehányásokat tenni. Bánffy Dénes Telekinek: „Kegyelmed ír az én clavissal írt levelembeli fogyatkozásrúl; talán az sem volt a nélkül, de bizony igazán vak nevet világtalant. Turpe est doctori..."[141]

Kódtörés

A kora újkori kódolók és dekódolók korántsem tettek meg minden óvintézkedést, hogy a lelepleződést és a rejtjelezett üzenet kitudódását elkerüljék. Vajon mennyire használta ki óvatlanságukat az ellenfél? Milyen kódtörő szakemberek és irodák szerveződtek a múltban az ellenséges kódok feltörésére, és vajon milyen eszközökkel dolgoztak? A kérdés az alábbiakban tehát nem az, hogyan folyt a dekódolás – azaz a rejtjelezett levelek nyílt szöveggé alakítása baráti személy által a kulcs birtokában –, hanem, hogy milyen eszközök álltak a kódtörést – a kulcs nélküli, pontosabban a kulcs rekonstruálását célzó gyakorlatot – folytató ellenséges személy rendelkezésére. Azaz hogyan nézett ki a kora-újkorban a kriptanalízis tudománya.[142] A téma jellegéből fakadóan jelentősen kevesebb adatunk, forrásunk, rekonstruálható megjegyzésünk van erre nézve, mint a kódolás eddig ismertetett gyakorlatát követően.

A kódtörési kézikönyvek a 15–17. században ritka madárnak számítottak. Azok közülük, amelyek a halandó ember számára is hozzáférhetők voltak, mindig gondosan vigyáztak ar-

[137] 1660. július 26. Teleki 1. 538–539., 459. sz.

[138] Thaly Kálmán (szerk.): *Késmárki Thököly Imre és némely főbb hívének naplói és emlékezetes írásai, 1686–1705*. Monumenta Hungariae Historica 2. Scriptores 23. Pest, 1868. 187.

[139] Benda: *Ráday Pál iratai*, 502.

[140] Idézi: Benda: *Ráday Pál iratai*, 505. Eszerint Pápai válasza a G. 15. Caps. C. Fasc 33-ban található, én azonban a Fasc 36-ban azonosítottam a kéziratot és az adott mondatot (fol. 27v).

[141] 1662. február 16. Teleki 2. 244–247., 182. sz.

[142] A kriptanalízis (cryptanalysis) modern keletkezésű szó, William Friedman, a 20. század első felének nagy kódfejtője alkotta.

ra, hogy a legmodernebb kódok feltörési módszereit titokban tartsák. Számos közülük csak a korukban már elavult módszerek feltöréséhez nyújt segítséget, így a milánói államférfi, Cicco Simonetta kódfejtő szabálygyűjteménye 1474-ből: *Regule ad extrahendum litteras ziferatas sine exemplo,*[143] vagy Antonio Maria Cospinek, a toszkánai herceg titkárának 1641-os könyve.[144] Más szerzők, mint François Viète (1540–1603), jogász matematikus és IV. Henrik zseniális kódfejtője[145] vagy a kora újkor legrészletesebb és legdidaktikusabb kódfejtő kézikönyve, a *Desifrírozás művészete (Art de deschiffrer)*[146] már hasznosabb módszereket kínál, amelyeket elsajátítva a figyelmes olvasó a siker reményében támadhat meg egy akkori titkosírást.

Ezek a szövegek nem voltak elérhetők a kora újkor Magyarországán. Jó eséllyel feltételezhetjük azonban, hogy a gyakoroló kódfejtőknek hasonló módszerek állhattak rendelkezésére az elfogott ellenséges titkosírások feltöréséhez. Sőt, a források arra utalnak, hogy – intellektuális szempontból – szerényebb eszközök voltak használatban, úgymint az üzenet továbbítójának a kivallatása vagy a titkosíráskulcs – rekonstruálás helyetti – megszerzése.

Így például a „Wesselényi összeesküvés" során használt *clavis*ok egy része igen elavult, monoalfabetikus volt,[147] így megfejtésük nem jelenthetett komoly gondot az udvarnak, kódfejtésről mégsem tudunk, az összeesküvők kulcsainak lefoglalása azonban mind Széchy Mária nádorné iratai közül, mind Szenthe Bálint Nádasdyval folytatott levelezéséből a szervezkedés felgöngyölítésének fontos részét képezte.[148]

A titkos levelezés megfejtésének más esetekben is inkább fizikai, mint intellektuális útjait járták, a levélvivő vagy a kém vallatása, kivégzése és leveleinek, kulcsainak elvétele tűnt a legpraktikusabb eszköznek. Pápai János és Teleki Mihály 1709-es drinápolyi követségének naplójából az derül ki, hogy a pasával való tárgyalás során is a tervezett kapcsolattartás biztonsága okozott aggodalmat: „Az levél által való correspondentiárúl gondolkoztunk." Mit bízhatnak *clavis*ra, mihez szükséges külön titkos követet küldeni, félő-e, hogy a követet tortúrának vetik alá?[149]

---

[143] Meister: *Die Anfänge der modernen diplomatischen Geheimschrift,* 61–63. Simonetta szövegének angol fordítása és elemzése: Buonafalce, Augusto: *Cicco Simonetta's Cipher-Breaking Rules.* Cryptologia, 32. (2008) 62–70. Simonettához lásd még: Simonetta, Marcello: *The Montefeltro Conspiracy: A Renaissance Mystery Decoded.* London, 2008.

[144] Cospi, Antonio Maria: *L'interpretation des chiffres ou reigle pour bien entendre et expliquer facilement toutes sortes de chiffres simples.* Paris, 1641. A könyvet Cospi olasz nyelvű eredeti szövegéből F.I.F.N.P.M. (Niceron atya) fordította franciára.

[145] Pesic, Peter: *François Viète, Father of Modern Cryptanalysis – Two New Manuscripts.* Cryptologia, vol. 21. (1997) 1–29.

[146] Devos, Jerôme Pierre – Seligman, Herbert (dir.): L'art de déchiffrer. Traité de déchiffrement du XVIIe siècle de la *Secrétairerie d'Etat et de Guerre Espagnole.* Leuven, 1967.; lásd még: Seligman, H.: *Un traité de déchiffrement du XVIIe siècle.* Revue des Bibliothèques et Archives de Belgique, 6 (1908) 1–19.

[147] A Haus-, Hof- und Staatsarchivban fennmaradt huszonhárom kulcs közül tíz monoalfabetikus vagy gyenge homofonikus: ÖStA HHStA Ungarische Akten Specialia Verschwörerakten VII. Varia (Pressburger Kommission etc.) Fasc. 327. Konv. D. Chiffres 1664-1668, fol 1- 61. Lásd még Wesselényi Ferenc két rejtjeles, monoalfabetikus fogalmazványát: MOL. E 199. 8. csomó, 1. pallium.

[148] Pauler Gyula: *Wesselényi Ferencz nádor és társainak összeesküvése: 1664–1671.* Budapest, 1876. 2. köt. 133–134., 165–166.

[149] Thaly Kálmán (közli) - Monumenta Hungariae Historica 2. Scriptores 27.: Történelmi naplók, 1663–1719. Budapest, 1875. - Gr. Teleki Mihály és Pápai János nándor-fejérvári követségének diariuma. 1709. 240–241.

Rákóczi katonai törvénykönyvében, a majd Ónodon becikkelyezendő *Regulamentum universalé*ban külön is rendelkezik az ellenséggel való *correspondentia* tilalmáról, valamint az ellenség levelének elfogási, megállítási kötelezettségről: „Titulus VI, Articulus XIII, *Az ellenséggel valaki correspondentiáját tudók s meg nem jelentők büntetése:* Aki az ilyen correspondentiákat meg tudja s az ellenségnek jött levelét kezéhez nem veszi vagy meg nem hallja s meg nem jelenti a tiszteknek, vagy meg nem adja vagy küldi, vagy a kémeket s a féle levélhordozókat hallja, s hírré nem adja, meg nem fogja és minden javokkal kezünkhöz vagy generalissinkhoz nem küldi, meg hal érette." Valamint: „Articulus XXIII, *Az ellenség leveleit senki ne folytassa,* Ellenségink akár mely leveleit senki ne folytassa, hanem reá találván, magunk vagy közelebb való generálisunk kezéhez hozza, mert másként mind az ki folytatja s mind aki megtudja, hogy valakinél oly levél vagyon s meg nem jelenti, mint áruló úgy büntettetik."[150]

Vallomásaiban az 1706-os év alatt Rákóczi megemlékezik arról, hogy éppen egy elfogott levelet saját maga megfejtve ismerte meg a császár Rabutinhoz intézett utasítását.[151] 1708-cal kapcsolatban pedig egy ellenséges titkár elfogását említi, akinél egy Heister tábornokhoz küldött titkosíráskulcsot találtak. Bercsényi Miklós 1705 és 1706 folyamán több, a fejedelemhez írott levelében is említ elfogott, „intercipiált" *clavis*os leveleket, amelyek tartalmát igyekszik kitalálni.[152]

A szabadságharc irattárában legalább tíz olyan német nyelvű, gót betűs *clavis* is fennmaradt (Rabutintól a császárnak és a „kolozsvari commendansnak", Glöckelsperg tábornok szatmári várparancsnoktól az Udvari haditanácsnak, más császári tábornokoktól és városparancsnokoktól egymás közt stb.), amelyek a császári oldal kommunikációját titkosították. Ezek egy részét feltehetően elfogott levelek alapján rekonstruálták a fejedelem titkárai, néhány azonban alacsonyabb színvonalú köztük, ezért az sem zárható ki, hogy nem elfogott kulcsok, hanem olyan, kevéssé bonyolult módszerek, amelyeket sikerült feltörni.[153]

Természetesen a másik oldalról nézve az okozott aggodalmat, vajon nem állítja-e meg az ellenfél a saját leveleket, nem tulajdonítja-e el a *clavis*okat. Ébeni István Teleki Mihálynak 1662-ben és 1663-ban írt leveleiben két ízben is említi levelek módszeres fogdosását, az első alkalommal arról is szól, hogy az elfogott levelek alapján a *clavis*ok kitudhatók.[154] Teleki felesége, Véér Judit 1662. május 30-án írt rövid, titkosítatlan leveléhez egy teljesen sifrozott utószót fűz, amelyben egy elfogott és felakasztott levélvivőt említ: „Ha Kegyelmed innét rég elindult volna, elfogták volna az puskások. Az szelniczei jobbágyot, az ki levelet vitt Szamosujvárra, elfogták, Apafinak vitték, az török felakasztatta."[155] Bánffy Dénes maga sérti meg a levéltitkot, és küldi a kitudott információt *clavis*sal Telekinek (sőt, az uralkodó és az érsek leveleinek felbontását is csak titkosítva – alább dőlten – vallja be): „Váczi püspök uram bemenetelinek micsoda gyümölcse lött, mindnyájan szomorúan érezhetjük, ki féltében-e? inexperientiábúl-e? megcsinálásbúl-e? egészlen az török pártjára állott, és ret-

[150] *Regulamentum universale, inclytorum confoederati regni Hungariae statuum ac ordinum, tam militarium, quam et ex parte inclytorum comitatuum, liberarum item ac regiarum civitatum, aliorumque quorumvis, observandum.* Nagyszombat, 1707. RMK I. 1733., idézi: Révay: *II. Rákóczi Ferenc,* 14–15. Lásd még: Ságvári György: *A kuruc hadsereg és a Regulementum Universale: hadszervezés és hadellátás Ónod után.* Hadtörténelmi Közlemények, 120. évf. (2007) 4. sz. 1352–1364.

[151] Idézi: Révay: *II. Rákóczi Ferenc,* 14., 98.

[152] AR I. oszt. 4. köt. 374–375., 61. sz. és AR I. oszt. 5. köt. 100–104 (38. sz.); 120–122 (53. sz.).

[153] Mol G 15 Caps. C. Fasc 43. másolatuk kiadva: Révay: *II. Rákóczi Ferenc,* 90–95.

[154] Teleki 2. 396–397., 293. sz. és Teleki 2. 436–437., 320. sz.

[155] Teleki 2. 294–295., 223. sz.

tenetes zelussal adorálja, kényszeríti ő felségét, vigye ki az várakbúl az praesidiumokat, mert Ali pasa azt írta, hogy mind megveszi stb., azért elvesz Erdély; *melyet, az érseknek írt levelét felszakasztván, abbúl az ő felségének írt levelének páriáját is kivevén, tanultunk ki, melyet* clavisra fordítván, Kegyelmednek elküldtünk."[156] Czegei Vass György naplójában 1704 márciusának eseményeihez azt jegyzi fel, hogy a leveleire leselkedő veszélyt konstatálván *clavist* küldött, így ha elfogják leveleit, akkor se tudják elolvasni őket, de aztán (bár a szövege nehezen érthető), úgy tűnik, a *clavi*sait is elfogták.[157] Koháry István 1678-ban Tököli leveleinek sikeres elfogásáról ír Esterházy Pál nádornak, de láthatóan nincsen eszköze arra, hogy a titkosított leveleket feltörje: „Akarám ezen alkalmatossággal Nagyságodnak alázatossan szolgai kötelességem szerint értésére adnom hogy bizonyos csomó leveleket intercripiálván katonáim (mellyeket részint Grroff Tököli táborárul vittek volna *Kővárra*, s részint Kővárbul hoztanak volna *Tököli* úrfinak), felszaggattam. De minthogy számvető czifrákkal irták jobjára egész leveleiket, semmi ollyast nem tanulhattam belőlök. Valóságos derék leveleknek kell lenni."[158]

Esetenként azonban mégsem ülnek ölbe tett kézzel, amíg meg nem szerzik a megfelelő kulcsot. Ha nem is állnak neki a kód megfejtésének, legalább igyekeznek a forgalomanalízis alapján (azaz, ki mikor kinek küldte a levelet) vagy pedig a sifrírozatlan levélrészből, esetleg más levelekből kikövetkeztetni a sifrírozott tartalmat. Teleki Mihály Rhédey Ferencnek írt 1677-es levelében mindkét módszert említi,[159] sőt 1664. november 27-én Apafinak írt levelében maga is gyakorolja a forgalomanalízist, bár Rottal és a havasalföldi vajda *clavis*os leveleit elolvasni nem tudja, magából a levélváltás tényéből és jellegéből le tud vonni következtetéseket: „Mint tractáltanak legyen itt Rottal urammal ő nagyságával, én bizonyosan nem tudom, eltitkolván azt tűlem, de az bizonyos, hogy ezen mostan kijött vajda embere sok clavissal írt levelet hozott ezen követnek; valóban suttogtanak is mind az jesuitával, ki által ezelőtt is tractálta minden dolgait az vajda, és amaz phariseus pater Kászonival. Nekem ugyan tegnap maga Rottal uram ő nagysága azt mondá, ezen vajda követjét is ő nagyságára relegálták, igéré is, hogy velem is mindazokat communicálni fogja, mely ha leszen, én is Nagyságodat alázatosan sietséggel igyekezem tudósítanom."[160]

Korszerűség vagy elmaradottság

Jogosan vetődik fel a kérdés, mennyire volt a magyarországi titkosírás-használat korszerű, *„up to date"* az adott kor európai rejtjeltechnikájához képest. A vizsgálatnak ezen a fokán, a *clavis* táblázatokat és a sifrírozott leveleket átvizsgálva talán választ adhatunk erre a kérdésre. Az első benyomásunk pozitív lehet: amennyiben összehasonlítjuk a Rákóczi-szabadságharc legjobb tábláit a kor más rejtjelkulcsaival a császári államkancellária,[161] a pápai

[156] Teleki 2. 309–311., 233. sz.

[157] Nagy Gyula (szerk.): *Czegei Vass György naplói.* Monumenta Hungariae Historica 2. Scriptores 35.: Magyar történelmi évkönyvek és naplók a XVI–XVIII. századokból. III. Budapest, 1896. 391–392.

[158] Merényi Lajos: *Kohary István levelei Eszterházy Pál nádorhoz. 1670–1682.* MTT IV. 4. köt. 67–82., különösen: 81–82.

[159] Teleki 7. 563–565., 393. sz.

[160] Teleki 3. 283–286., 231. sz.

[161] ÖStA HHStA Staatskanzlei Interiora Kt. 13-16. Chiffrenschlüssel. Az anyaghoz lásd még a MOL könyvtárában megtalálható segédletet: V/5/2-4 *Staatskanzlei: Vorträge: Interiora und Provinzen*, 16–28.

diplomácia[162] vagy a francia udvar[163] *clavis*aival, akkor azt látjuk, hogy sem méretben (a betűknek, szótagoknak, nomenklatoroknak megfeleltetett számok mennyiségében), sem szerkezetben (végiggondolt, nullitásokkal kiegészített homofonikus jellegében) nincsen szégyenkezni valójuk.

A gondosabb vizsgálat azonban kissé árnyalja a képet. Először is, a fejedelmi diplomáciának éppen azok a levelezési irányai képviselték a legnagyobb fejlettségi szintet, amelyek a franciáknak köszönhetően formálódtak: a francia udvar küldte azokat a táblákat, amelyekkel Rákóczi felzárkózott a nemzetközi szintre. A 17. században Richelieu, majd XIV. Lajos matematikus-kriptográfusa, Antoine Rossignol (1590–1673) kidolgozta azt a hatalmas, 590 elemből álló homofonikus, szótagokat titkosító rendszert, ami aztán a *„Grand Chiffre"* nevet kapta, és amelyet aztán kétszáz évig, Étienne Bazeries-ig (1846–1931) senki nem tudott megfejteni.[164] Természetesen nem ezt kínálta fel a Napkirály udvara keleti szövetségesének, hanem az akkori legfejlettebb módszerüket. Ez azonban még mindig a kor legkomolyabb táblái közé tartozott.

Rákóczi környezetében hasonló kidolgozást nyert számos követ *clavis*a (így a fentebb tárgyalt Pápai-féle tábla is), azonban a szabadságharc „helyi érdekeltségű" rejtjelei meglepően primitívek maradtak. Károlyi Sándor és Bercsényi Miklós 1705-ös *clavis*a például nemcsak, hogy monoalfabetikus, de ráadásul grafikus jelekkel is működik. E jelek használata egészen biztosan nem segítette, hogy a csatamezőn gyorsan és egyértelműen kommunikáljanak. A helyett négyzetet, b helyett háromszöget, e helyett egy 'm' alakú jelet a végén kereszttel rajzolni igencsak körülményes, de gondolhatunk arra is, mennyivel nehezebb kikeresni egy táblázatból egy sehogy sem osztályozható jelet, mint egy sorba rendezhető számot.[165] Márpedig egy sor levél bizonyítja, hogy e kevéssé praktikus tábla bizony használatba is került.[166] Ugyanilyen gyenge – grafikus jelekkel működő monoalfabetikus – Rákóczi és Bercsényi 1704-es *clavis*a,[167] amelyről biztosan nem állíthatjuk, hogy lényegtelen információk cseréjére használták volna, hiszen talán ez a levelezési irány volt a szabadságharc legfontosabb kommunikációs útvonala.[168] Szintén monoalfabetikusak és szintén jelekből állnak Hentér Mihály konstantinápolyi követnek 1707-ben a fejedelemhez küldött levelei.[169] Egyszóval a fejedelmi diplomácia rejtjelgyakorlatának fejlettsége egyenetlen, a magas fejlettség inkább jellemző a nemzetközi viszonylatra, mint a belföldire, ami gyakran kevésbé volt praktikus.

---

[162] Meister: *Die Geheimschrift.* Ebben az esetben az összehasonlítás nem tökéletes, a kötet ugyanis megáll a 16. század végi tábláknál, azonban a pápai udvar *clavis*ainak kidolgozottsága nem változik jelentősen a következő kétszáz év során. Lásd: Alvarez, David: *The Papal Cipher Section In The Early Nineteenth Century.* Cryptologia, vol. 17 (1993) 219–224.

[163] Lerville, Edmond: *Les cahiers secrets de la cryptographie.* Párizs, 1972.; Sacco, L.: *Manuel de Cryptographie.* Paris, 1951.

[164] Lerville: *Les cahiers secrets,* 64–74.; Commandant Bazeries: *Les chiffres secrets dévoilés, étude historique sur les chiffres appuyée de documents inédits tirés des différents dépôts d'archives.* Paris, 1901.; Kahn, David: *The Man with the Iron Mask: Encore et Enfin: Cryptologically.* Cryptologia, vol. 29 (2005) 43–49.

[165] Hadtörténeti Levéltár E. 1705/18.

[166] Hadtörténeti Levéltár E. 1705/5, 6, 03, 16, 17.

[167] Rekonstruálva: AR I. oszt. 4. köt. Melléklet.

[168] Lásd egy sor 1708-as levelet, például: AR I. oszt. 2. köt. 163–167., 10. sz., 13. sz. 28. sz. stb.

[169] Mol G 15 Caps. D. Fasc 80. fols. 38, 40, 46. Ugyanennek a kódnak az 1708-as használatához lásd: Mol G 15 Caps. E. Fasc 109.

A másik megfigyelés, ami árnyalja a képet, az, hogy a magyarországi rejtjelhasználat a nyugat-európaival összehasonlítva lassabban ért el ugyanarra a fejlettségi szintre, és még a 17. század közepén és végén is meglepően egyszerű módszereket látunk olyan esetekben is, ahol az információ elrejtése élet és halál kérdése volt.

I. Rákóczi György 1637. február 2-án például kedélyesen írja követének, Tholdalaghi Mihálynak: „Kegyelmednek többet írnánk, de pennára nem bízhatjuk, hanem ím egy clavist küldtünk be, ezután ezzel írunk. Ebben csak az az mesterség, hogy az felső 12 betűt az alsóval kell kiírni, az alsó 12 betűt meg az felsővel."[170] Magyarul, a fejedelem a kriptográfiatörténet talán legegyszerűbb módszerét ajánlja, az ábécé első felének betűit kölcsönösen megfeleltetjük az ábécé második felének. Nomenklatorok, nullitások, szótagok és homofónok nincsenek. És ha kétségeink volnának, hogy ezt a módszert valóban alkalmazta-e, a kétségek eloszlanak, ha végigolvassuk az Ötvös Ágoston szerkesztésében 1848-ban megjelent rejtelmes leveleket, amelyek jelentős részét e sérülékeny módszerrel titkosította a fejedelem.[171] A kötetben szereplő sifrírozott leveleket összesen hat különböző kulccsal titkosították, ezek közül csupán kettő homofonikus *clavis*, négy monoalfabetikus. Magyarul, a fejedelem *clavis*ainak nagyobb részét egy iskolás is fel tudta törni.

Maradva az erdélyi környezetnél, néhány évvel később hasonló furcsasággal szembesülünk. Az akkori fejedelemmel, II. Rákóczi Györggyel levelező Mednyánszky Jónás 1655 és 1658 közt egy tisztességes homofonikus rendszert használ leveleiben.[172] A több jegyzetlapon is fennmaradt rendszerben három szám felel meg minden betűnek, a szótagok helyett külön számok állnak, és néhány nomenklator egészíti ki a rendszert (191 – Rex Hung v. Király, 346 – Moldavia, 294 – Papista, 347 – Transalpina, 366 – Russia, 192 – Palatinus, 194 – Primas, 204 – Svecus, 193 – judex curiae).[173] 1658-ban azonban leveleikben[174] áttérnek egy egyszerűbb kulcsra, amely monoalfabetikus, és grafikus jelekből, betűkből, valamint számokból áll. Nincsenek benne szótagok, csupán hat nomenklator árválkodik a lap végén (4 – Nádasdy, X – Érsek, 10 – Porta ottomanica, Z – Rákóczy, W – Cancellar, 271 – Király, N – Palatinus).[175] Mi lehetett az okuk, hogy egy viszonylag fejlettebb *clavis*t egy meglehetősen elmaradottra és nehézkesre cseréltek? Legalább ilyen meghökkentő, hogy a Wesselényi összeesküvésben használt egyes levelek[176] és egyes táblák[177] is monoalfabetikusak.

Félrevezető lenne természetesen azt a benyomást kelteni, hogy a magyarországival ellentétben a nyugati rejtjelhasználat egyenletesen magas színvonalon folyt volna. A legkevésbé sem volt így, a kétségtelenül nagyszámú és magas színvonalú *clavis* mellett találunk meglepő kivételeket. II. Ferdinánd császár 1621-ben Jacobus Curtis (Jakob Kurtz) lengyel-

[170] Beke Antal – Barabás Samu (szerk.): *I. Rákóczi György és a porta.* Budapest, 1888. 340–341.

[171] Ötvös Ágoston: *Rejtelmes levelek,* A rejtelmes kulcsok ismertetése. Lásd még: Révay: *Titkosírások,* 76–86.

[172] MOL E 190, Archivum familiae *Rákóczi,* 43. doboz, 5 tétel, pl 794, 802. 816. 821. 872. 875. 886. sz.

[173] MOL P 497 Mednyánszky Család, 3. csomó, Kulcsok II. Rákóczy György és Mednyánszky Jónás levelezéséhez, fol. 13, 5, 2, 4.

[174] MOL E 190, Arch Fam. Rakóczi, 44. doboz, 5 tétel, pl 891-893, 897-8, 901, 904, 909, 924, 926.

[175] MOL P 497 Mednyánszky Család, 3. csomó, Kulcsok II. Rákóczy György és Mednyánszky Jónás levelezéséhez, fol. 11-12.

[176] Monoalfabetikus módszerrel titkosított levelek: MOL E 199. 8. csomó, 1. pallium.

[177] Monoalfabetikus táblák: ÖStA HHStA Ungarische Akten Specialia Verschwörerakten VII. Varia (Pressburger Kommission etc.) Fasc. 327. Konv. D. Chiffres 1664–1668, fol. 17, fol. 32, fol. 39, fol. 54, fol. 55.

országi megbízottjával egy monoalfabetikus *clavis*t használva levelezik.[178] III. Ferdinánd császárnak Johann Ludwig Kuefstein, portai követ 1628–1629-ben grafikus jelekkel sifrírozva ír (ráadásul igen gyenge, majdnem monoalfabetikusnak számító homofonikus módszerrel).[179] Miként a császári udvarnak jelentő titkos levelezők, azaz kémek 1632-ben írt olasz nyelvű levelüket is grafikus jelekből álló *clavis*okkal titkosítják.[180] Hatvan évvel korábban még bevett volt a császári adminisztrációban a grafikus jelek használata (például Carolus Rym, konstantinápolyi leveleit 1571 körül így titkosítja),[181] a 17. században azonban már a kezelhetőbb számok dominálnak. Hosszan lehetne még sorolni hasonló kivételeket, amelyek azt bizonyítják, a fejlődés az osztrák császári kormányzat gyakorlatában sem volt lineáris, és hogy a történelmi szereplők nem feltétlenül azt érezték fejlettebbnek és praktikusabbnak, amit mi ma annak vélünk.

Összességében megállapíthatjuk, hogy vizsgálati korszakunk végére a magyarországi titkosírás-használat lényegében felzárkózott a közép- és nyugat-európaihoz, azonban ezt elsősorban éppen a nyugati gyakorlat hatására tette. Ha a felzárkózás folyamatát vizsgáljuk, azt látjuk, hogy ez kissé megkésett volt, az Erdélyi Fejedelemség rejtjelhasználata a 17. század közepén igencsak messze állt a Habsburg követek *clavis*ainak szintjétől, és Teleki Mihálynak is csak egyes táblái álltak nyugati színvonalon, míg számos továbbra is monoalfabetikus maradt.[182] Az a gyakorlat pedig, hogy mind I. Rákóczi György, mind II. Rákóczi Ferenc számára természetes volt, hogy maga clavisáljon, semmiképpen nem nevezhető fejlett titkosírás-használatnak. Azaz fejlett módszert is lehet fejletlen módon használni.

[178] A levél: HHStA, Ung Akt. Misc Fasc 422 Conv 1 fol 72-79., a tábla: uo. fol. 75.

[179] ELTE Egyetemi könyvtár, G. 4. Fol. Tom. V. 469–958. Lásd még: Donáth Regina: *A diplomáciai titkosírás XVII. századi használatához.* Magyar Könyvszemle, 80. évf. (1964) 1. sz. 55–62.

[180] ÖStA HHStA Staatenabteilungen Türkei I. Kt. 112. Konv. 5. fol. 1–4. (eredeti); 5–9. (desifrírozott); valamint fol. 17–23. (desifrírozott); fol. 24–28. (eredeti). A forrásokra Kerekes Dóra hívta fel a figyelmem, amiért ezúton mondok köszönetet.

[181] ÖStA HHStA Türkei I. Karton 28. Konv. 1. 1571. fol. 33-87, 44-47, 52-54, 65-66.

[182] MOL. P 1238 Teleki Mihály Gyűjtemény. Vegyes Iratok. Titkosírás kulcsok

BENEDEK LÁNG

The technology of cryptography in Hungary around 1700

Sixteenth and seventeenth century ciphered messages are rich information resources of their age. The historian can get close to the attitude of the people involved, to their notion of secret and to the details of their use of technology.

What was the relationship of – often civilian – users to the technology they used: did they understand how it worked, did they realize its potentials? How much did they trust that the coded texts will remain secret? To what extent were the people involved in the political and military conflicts aware that their ciphered letters may be deciphered? To what extent were the potentials of a code exploited, to what extent did they endanger the security of information with their carelessness? What typical mistakes did they make and what kind of misunderstandings resulted from these? Were they familiar with the decoding technology of the enemy? Did they make efforts to protect a coding method from being discovered? Did they change their codes often enough? Was any given political player careful enough to use different codes with their different corresponding partners? Who did the ciphering, the head chancellor or the prince himself? And who did the deciphering? Can we reconstruct with the help of the sources what methods were used to break a code?

The article offers a systematic analysis of the use of cipher systems and enciphered messages survived from the Hungarian history around 1700.